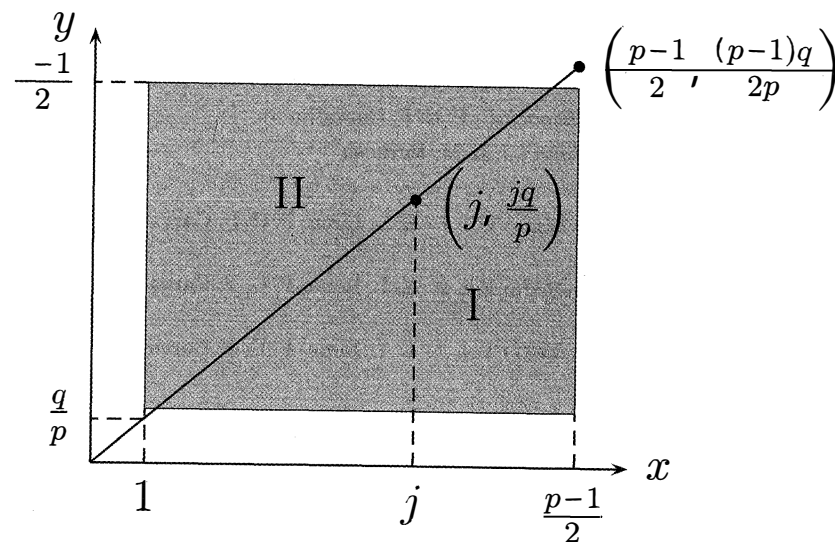
Distribuição e vendas
Sociedade Brasileira de Matemática
Estrada Dona Castorina, 110 Sala 109 - Jardim Botânico
22460-320 Rio de Janeiro RJ
Telefones: (21) 2529-5073 / 2529-5095
http://www.sbm.org.br / email:lojavirtual@sbm.org.br

ISBN 978-85-85818-87-6

MUNIZ NETO, Antonio Caminha.
Tópicos de Matemática Elementar: teoria dos números / Caminha Muniz
-2.ed. -- Rio de Janeiro: SBM, 2013.
v.5 ; 263p. (Coleção Professor de Matemática; 28)
ISBN 978-85-85818-87-6

1.Divisibilidade. 2. Equações Diofontinas.
3. Cálculo e Teoria dos Números. I. Título

Tópicos de Matemática Elementar
Volume 5
Teoria dos Números

Antonio Caminha Muniz Neto

2ª edição
2ª impressão
2014
Rio de Janeiro

COLEÇÃO DO PROFESSOR DE MATEMÁTICA

COLEÇÃO DO PROFESSOR DE MATEMÁTICA

- *Logaritmos* - E. L. Lima
- *Análise Combinatória e Probabilidade com as soluções dos exercícios* - A. C. Morgado, J. B. Pitombeira, P. C. P. Carvalho e P. Fernandez
- *Medida e Forma em Geometria (Comprimento, Área, Volume e Semelhança)* - E. L. Lima
- *Meu Professor de Matemática e outras Histórias* - E. L. Lima
- *Coordenadas no Plano com as soluções dos exercícios* - E. L. Lima com a colaboração de P. C. P. Carvalho
- *Trigonometria, Números Complexos* - M. P. do Carmo, A. C. Morgado e E. Wagner, Notas Históricas de J. B. Pitombeira
- *Coordenadas no Espaço* - E. L. Lima
- *Progressões e Matemática Financeira* - A. C. Morgado, E. Wagner e S. C. Zani
- *Construções Geométricas* - E. Wagner com a colaboração de J. P. Q. Carneiro
- *Introdução à Geometria Espacial* - P. C. P. Carvalho
- *Geometria Euclidiana Plana* - J. L. M. Barbosa
- *Isometrias* - E. L. Lima
- *A Matemática do Ensino Médio Vol. 1* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *A Matemática do Ensino Médio Vol. 2* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *A Matemática do Ensino Médio Vol. 3* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *Matemática e Ensino* - E. L. Lima
- *Temas e Problemas* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *Episódios da História Antiga da Matemática* - A. Aaboe
- *Exame de Textos: Análise de livros de Matemática* - E. L. Lima
- *A Matemática do Ensino Medio Vol. 4 - Exercicios e Soluções* - E. L. Lima, P. C. P. Carvalho, E. Wagner e A. C. Morgado
- *Construções Geométricas: Exercícios e Soluções* - S. Lima Netto
- *Um Convite à Matemática* - D.C de Morais Filho
- *Tópicos de Matemática Elementar - Volume 1 - Números Reais* - A. Caminha
- Tópicos de Matemática *Elementar - Volume 2 - Geometria Euclidiana Plana* - A. Caminha
- *Tópicos de Matemática Elementar - Volume 3 - Introdução à Análise* - A. Caminha
- *Tópicos de Matemática Elementar - Volume 4 - Combinatória* - A. Caminha
- *Tópicos de Matemática Elementar - Volume 5 - Teoria dos Números* - A. Caminha

A meus filhos Gabriel e Isabela,
na esperança de que um dia leiam este livro.

Sumário

Prefácio à primeira edição

Prefácio à segunda edição

1 Divisibilidade **1**
- 1.1 O algoritmo da divisão 2
- 1.2 MDC e MMC 13
- 1.3 Números primos 35

2 Equações Diofantinas **51**
- 2.1 Ternos Pitagóricos 51
- 2.2 A equação de Pell 62

3 Funções Aritméticas Multiplicativas **73**

4 Cálculo e Teoria dos Números **91**
- 4.1 Sobre a distribuição dos primos 91
- 4.2 O teorema de Chebyshev 99
- 4.3 O teorema de Cèsaro 105

5 A Relação de Congruência **117**
5.1 Definições e propriedades básicas 118
5.2 Os teoremas de Euler e Fermat 133
5.3 Congruências lineares e o teorema chinês dos restos . . 145

6 Classes de Congruência **153**
6.1 Sistemas de restos 153
6.2 O conjunto quociente $\mathbb{Z}_n$ 161

7 Raízes Primitivas e Resíduos Quadráticos **169**
7.1 Ordem módulo n 170
7.2 Raízes primitivas 175
7.3 Resíduos quadráticos 187
7.4 Somas de quadrados 202

8 Sugestões e Soluções **209**

Referências **241**

A Glossário **243**

Prefácio à primeira edição

Esta coleção evoluiu a partir de sessões de treinamento para olimpíadas de Matemática, por mim ministradas para alunos e professores do Ensino Médio, várias vezes ao longo dos anos de 1992 a 2003 e, mais recentemente, como orientador do Programa de Iniciação Científica para os premiados na Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) e do Projeto Amílcar Cabral de cooperação educacional entre Brasil e Cabo Verde.

Idealmente, planejei o texto como uma mistura entre uma iniciação suave e essencialmente autocontida ao fascinante mundo das competições de Matemática, além de uma bibliografia auxiliar aos estudantes e professores do secundário interessados em aprofundar seus conhecimentos matemáticos. Resumidamente, seu propósito primordial é apresentar ao leitor uma abordagem de quase todos os conteúdos geralmente constantes dos currículos do secundário, e que seja ao mesmo tempo concisa, não excessivamente tersa, logicamente estruturada e mais aprofundada que a usual.

Na estruturação dos livros, me ative à máxima do eminente matemático húngaro-americano George Pólya, que dizia não se poder fazer

Matemática sem *sujar as mãos*. Assim sendo, em vários pontos deixei a cargo do leitor a tarefa de verificar aspectos não centrais aos desenvolvimentos principais, quer na forma de detalhes omitidos em demonstrações, quer na de extensões secundárias da teoria. Nestes casos, frequentemente referi o leitor a problemas específicos, os quais se encontram marcados com * e cuja análise e solução considero parte integrante e essencial do texto. Colecionei ainda, em cada seção, outros tantos problemas, cuidadosamente escolhidos na direção de exercitar os resultados principais elencados ao longo da discussão, bem como estendê-los. Uns poucos destes problemas são quase imediatos, ao passo que a maioria, para os quais via de regra oferto sugestões precisas, é razoavelmente difícil; no entanto, insto veementemente o leitor a debruçar-se sobre o maior número possível deles por tempo suficiente para, ainda que não os resolva todos, passar a apreciá-los como corpo de conhecimento adquirido.

O primeiro volume discorre sobre vários aspectos relevantes do conjunto dos números reais e de álgebra elementar, no intuito de munir o leitor dos requisitos necessários ao estudo dos tópicos constantes dos volumes subsequentes. Após começar com uma discussão não axiomática das propriedades mais elementares dos números reais, são abordados, em seguida, produtos notáveis, equações e sistemas de equações, sequências elementares, indução matemática e números binomiais; o texto finda com a discussão de várias desigualdades algébricas importantes, notadamente aquela entre as médias aritmética e geométrica, bem como as desigualdades de Cauchy, de Chebychev e de Abel.

Dedicamos o segundo volume a uma iniciação do leitor à geometria Euclidiana plana, inicialmente de forma não axiomática e enfatizando construções geométricas elementares. Entretanto, à medida em que o texto evolui, o método sintético de Euclides – e, consequentemente, demonstrações – ganha importância, principalmente com a discussão dos conceitos de congruência e semelhança de triângulos; a partir desse ponto, vários belos teoremas clássicos da geometria, usualmente ausentes dos livros-texto do secundário, fazem sua aparição. Numa terceira etapa, o texto apresenta outros métodos elementares usuais no estudo da geometria, quais sejam, o método analítico de R. Descartes, a trigonometria e o uso de vetores; por sua vez, tais métodos são utilizados tanto para reobter resultados anteriores de outra(s) maneira(s) quanto para deduzir novos resultados.

Prefácio à primeira edição

De posse do traquejo algébrico construído no volume inicial e do aparato geométrico do volume dois, discorremos no volume três sobre aspectos elementares de funções e certos excertos de cálculo diferencial e integral e análise matemática, os quais se fazem necessários em certos pontos dos três volumes restantes. Prescindindo, inicialmente, das noções básicas do Cálculo, elaboramos, dentre outros, as noções de gráfico, monotonicidade e extremos de funções, bem como examinamos o problema da determinação de funções definidas implicitamente por relações algébricas. Na continuação, o conceito de função contínua é apresentado, primeiramente de forma intuitiva e, em seguida, axiomática, sendo demonstrados os principais resultados pertinentes. Em especial, utilizamos este conceito para estudar a convexidade de gráficos – culminando com a demonstração da desigualdade de J. Jensen – e o problema da definição rigorosa da área sob o gráfico de uma função contínua e positiva – que, por sua vez, possibilita a apresentação de uma construção adequada das funções logaritmo natural e exponencial. O volume três termina com uma discussão das propriedades mais elementares de derivadas e do teorema fundamental do cálculo, os quais são mais uma vez aplicados ao estudo de desigualdades, em especial da desigualdade entre as médias de potências.

O volume quatro é devotado à análise combinatória. Começamos revisando as técnicas mais elementares de contagem, enfatizando as construções de bijeções e argumentos recursivos como estratégias básicas. Na continuação, apresentamos um apanhado de métodos de contagem um tanto mais sofisticados, como o princípio da inclusão exclusão e os métodos de contagem dupla, do número de classes de

equivalência e mediante o emprego de métricas em conjuntos finitos. A cena é então ocupada por funções geradoras, onde a teoria elementar de séries de potências nos permite discutir de outra maneira problemas antigos e introduzir problemas novos, antes inacessíveis. Terminada nossa excursão pelo mundo da contagem, enveredamos pelo estudo do problema da existência de uma configuração especial no universo das configurações possíveis, utilizando para tanto o princípio das gavetas de G. L. Dirichlet – vulgo "princípio das casas dos pombos" –, um célebre teorema de R. Dilworth e a procura e análise de invariantes associados a problemas algorítmicos. A última estrutura combinatória que discutimos é a de um grafo, quando apresentamos os conceitos básicos usuais da teoria com vistas à discussão de três teoremas clássicos importantes: a caracterização da existência de caminhos Eulerianos, o teorema de A. Cayley sobre o número de árvores rotuladas e o teorema extremal de P. Turán sobre a existência de subgrafos completos em um grafo.

Passamos em seguida, no quinto volume, à discussão dos conceitos e resultados mais elementares de teoria dos números, ressaltando-se inicialmente a teoria básica do máximo divisor comum e o teorema fundamental da aritmética. Discutimos também o método da descida de P. de Fermat como ferramenta para provar a inexistência de soluções inteiras para certas equações diofantinas, e resolvemos também a famosa equação de J. Pell. Em seguida, preparamos o terreno para a discussão do famoso teorema de Euler sobre congruências, construindo a igualmente famosa função de Euler com o auxílio da teoria mais geral de funções aritméticas multiplicativas. A partir daí, o livro apresenta formalmente o conceito de congruência de números em relação a um certo módulo, discutindo extensivamente os resultados usualmente constantes dos cursos introdutórios sobre o assunto, incluindo raízes primitivas, resíduos quadráticos e o teorema de Fermat de caracterização dos inteiros que podem ser escritos como soma de dois quadrados. O grande diferencial aqui, do nosso ponto de vista, é o calibre dos

exemplos discutidos e dos problemas propostos ao longo do texto, boa parte dos quais oriundos de variadas competições ao redor do mundo.

Finalmente, números complexos e polinômios são os objetos de estudo do sexto e último volume da coleção. Para além da teoria correspondente usualmente estudada no secundário – como a noção de grau, o algoritmo da divisão e o conceito de raízes de polinômios –, vários são os tópicos não padrão abordados aqui. Dentre outros, destacamos inicialmente a utilização de números complexos e polinômios como ferramentas de contagem e a apresentação quase completa de uma das mais simples demonstrações do teorema fundamental da álgebra. A seguir, estudamos o famoso teorema de I. Newton sobre polinômios simétricos e as igualmente famosas desigualdades de Newton, as quais estendem a desigualdade entre as médias aritmética e geométrica. O próximo tema concerne os aspectos básicos da teoria de interpolação de polinômios, quando dispensamos especial atenção aos polinômios interpoladores de J. L. Lagrange. Estes, por sua vez, são utilizados para resolver sistemas lineares de Vandermonde sem o recurso à álgebra linear, os quais, a seu turno, possibilitam o estudo de uma classe particular de sequências recorrentes lineares. O livro termina com o estudo das propriedades de fatoração de polinômios com coeficientes inteiros, racionais ou pertencentes ao conjunto das classes de congruência relativas a algum módulo primo, seguido do estudo do conceito de número algébrico. Há, aqui, dois pontos culminantes: por um lado, uma prova mais simples do fechamento do conjunto dos números algébricos em relação às operações aritméticas básicas; por outro, o emprego de polinômios ciclotômicos para provar um caso particular do teorema de Dirichlet sobre primos em progressões aritméticas.

Várias pessoas contribuíram ao longo dos anos, direta ou indiretamente, para que um punhado de anotações em cadernos pudesse transformar-se nesta coleção de livros. Os ex-professores do Departamento de Matemática da Universidade Federal do Ceará, Marcondes

Cavalcante França, João Marques Pereira, Guilherme Lincoln Aguiar Ellery e Raimundo Thompson Gonçalves, ao criarem a Olimpíada Cearense de Matemática na década de 1980, motivaram centenas de jovens cearenses, dentre os quais eu me encontrava, a estudarem mais Matemática. Meu ex-professor do Colégio Militar de Fortaleza, Antônio Valdenísio Bezerra, ao convidar-me, inicialmente para assistir a suas aulas de treinamento para a Olimpíada Cearense de Matemática e posteriormente para dar aulas consigo, iniciou-me no maravilhoso mundo das competições de Matemática e influenciou definitivamente minha escolha profissional. Os comentários de muitos de vários de ex-alunos contribuíram muito para o formato final de boa parte do material aqui colecionado; nesse sentido, agradeço especialmente à João Luiz de Alencar Araripe Falcão, Roney Rodger Sales de Castro, Marcelo Mendes de Oliveira, Marcondes Cavalcante França Jr., Marcelo Cruz de Souza, Eduardo Cabral Balreira, Breno de Alencar Araripe Falcão, Fabrício Siqueira Benevides, Rui Facundo Vigelis, Daniel Pinheiro Sobreira, Antônia Taline de Souza Mendonça, Carlos Augusto David Ribeiro, Samuel Barbosa Feitosa, Davi Máximo Alexandrino Nogueira e Yuri Gomes Lima. Vários de meus colegas professores teceram comentários pertinentes, os quais foram incorporados ao texto de uma ou outra maneira; agradeço, em especial, a Fláudio José Gonçalves, Francisco José da Silva Jr., Onofre Campos da Silva Farias, Emanuel Augusto de Souza Carneiro, Marcelo Mendes de Oliveira, Samuel Barbosa Feitosa e Francisco Bruno de Lima Holanda. Os professores João Lucas Barbosa e Hélio Barros deram-me a conclusão de parte destas notas como alvo a perseguir ao me convidarem a participar do Projeto Amílcar Cabral de treinamento dos professores de Matemática da República do Cabo Verde. Meus colegas do Departamento de Matemática da Universidade Federal do Ceará, Abdênago Alves de Barros, José Othon Dantas Lopes, José Robério Rogério e Fernanda Esther Camillo Camargo, bem como meu orientando de iniciação científica Itamar Sales de Oliveira Filho, leram partes do texto final e ofereceram várias sugestões. Os pareceristas indicados pela SBM opinaram decisivamente para que os livros certamente resultassem melhores que a versão inicial por mim submetida. O presidente da SBM, professor Hilário Alencar da Silva, o antigo editor-chefe da SBM, professor Roberto Imbuzeiro de Oliveira, bem como o novo editor-chefe, professor Abramo Hefez, foram sempre extremamente solícitos e atenciosos comigo ao longo de todo o processo de edição. Por fim, quaisquer erros ou incongruências que ainda se façam presentes, ou omissões na lista acima, são de minha inteira responsabilidade.

Por fim e principalmente, gostaria de agradecer a meus pais, Antonio Caminha Muniz Filho e Rosemary Carvalho Caminha Muniz, e à minha esposa Mônica Valesca Mota Caminha Muniz. Meus pais me fizeram compreender a importância do conhecimento desde a mais tenra idade, sem nunca terem medido esforços para que eu e meus irmãos desfrutássemos o melhor ensino disponível; minha esposa brindou-me com a harmonia e o incentivo necessários à manutenção de meu ânimo e humor, em longos meses de trabalho solitário nas madrugadas. Esta coleção de livros também é dedicada a eles.

FORTALEZA, JANEIRO de 2012

Antonio Caminha M. Neto

Prefácio à segunda edição

Para a segunda edição fiz uma extensa revisão do texto e dos problemas propostos, corrigindo várias imprecisões de língua portuguesa e de Matemática. Adicionei também alguns problemas novos, no intuito de melhor exercitar certos pontos da teoria, os quais não se encontravam adequadamente contemplados pelos problemas propostos à primeira edição. Diferentemente da primeira edição, nesta segunda edição as sugestões e soluções aos problemas propostos foram colecionadas em um capítulo separado (o capítulo 8, para este volume); adicionalmente, apresentei sugestões ou soluções a praticamente todos os problemas do livro.

Por fim, gostaria de aproveitar o ensejo para agradecer à comunidade matemática brasileira, em geral, e a todos os leitores que me enviaram sugestões ou correções, em particular, o excelente acolhimento desfrutado pela primeira edição desta obra.

FORTALEZA, MAIO de 2013

Antonio Caminha M. Neto

CAPÍTULO 1

Divisibilidade

Este capítulo é devotado ao estabelecimento das definições e propriedades elementares concernentes à *relação de divisibilidade* no conjunto dos números inteiros, enfatizando o algoritmo da divisão, a noção de máximo divisor comum e o papel fundamental desempenhado pelos números primos. Em que pese o caráter elementar dos argumentos utilizados para tal fim, encontraremos ao longo do caminho vários problemas e resultados interessantes, destacados, dentre esses últimos, a caracterização dada por Bézout para o máximo divisor comum de dois inteiros e o teorema de Euclides sobre a infinitude do conjunto dos números primos. Ao leitor interessado em aprofundar seus conhecimentos de teoria dos números para além do material que discutimos neste volume, sugerimos o clássico [5].

1.1 O algoritmo da divisão

Definição 1.1. Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b **divide** a, e escrevemos $b \mid a$, se existir $c \in \mathbb{Z}$ tal que $a = bc$. Caso b não divida a, escrevemos $b \nmid a$.

Seja b um inteiro não nulo. Se b dividir a, dizemos que b é um **divisor** de a, que a é **divisível** por b ou ainda que a é um **múltiplo** de b. Se $b \mid a$ e $b > 0$, então b é um **divisor positivo** de a. Note que todo inteiro não nulo é um divisor de si mesmo e de 0.

Exemplo 1.2. Um inteiro n é **par** se for um múltiplo de 2; caso contrário, n é **ímpar**. De acordo com a definição 1.1, os inteiros pares são precisamente os que podem ser escritos na forma $2k$, para algum $k \in \mathbb{Z}$, i.e., são os inteiros

$$\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots.$$

Os inteiros restantes, i.e.,

$$\ldots, -5, -3, -1, 1, 3, 5, \ldots,$$

são os ímpares. Assim, todo ímpar é igual a um par mais 1, de modo que podemos denotar um inteiro ímpar genérico escrevendo $2k + 1$, onde $k \in \mathbb{Z}$.

Exemplo 1.3. Dados a, b inteiros e k natural, temos que:

(a) Se $a \neq b$, então $(a - b) \mid (a^k - b^k)$.

(b) Se $a \neq -b$ e k for ímpar, então $(a + b) \mid (a^k + b^k)$.

Solução.
(a) Sabemos, do problema 2.1.18 do volume 1 que

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}).$$

Como $a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1} \in \mathbb{Z}$, basta usar a definição 1.1.

(b) Para k ímpar, recorrendo uma vez mais ao problema 2.1.18 do volume 1, temos a fatoração

$$a^k + b^k = (a + b)(a^{k-1} - a^{k-2}b + \cdots - ab^{k-2} + b^{k-1}),$$

com $a^{k-1} - a^{k-2}b + \cdots - ab^{k-2} + b^{k-1}$ também inteiro. É, pois, suficiente utilizar novamente a definição 1.1. ■

Exemplo 1.4. Prove que, para todo $k \in \mathbb{N}$, o número $10^k - 1$ é um múltiplo de 9.

Prova. Basta aplicar o item (a) do exemplo anterior: $10^k - 1 = 10^k - 1^k$ é divisível por $10 - 1 = 9$. Outras possibilidades são observar que

$$10^k - 1 = \underbrace{99\ldots9}_{k \text{ algarismos}} = 9 \cdot \underbrace{11\ldots1}_{k \text{ algarismos}},$$

claramente um múltiplo de 9, ou escrever

$$10^k - 1 = (9 + 1)^k - 1 = \sum_{j=0}^{k} \binom{k}{j} 9^{k-j} - 1 = \sum_{j=0}^{k-1} \binom{k}{j} 9^{k-j},$$

novamente um múltiplo de 9. ■

A proposição a seguir estabelece algumas propriedades básicas da relação de divisibilidade, as quais o leitor deve guardar para uso futuro.

Proposição 1.5. Sejam a, b, c inteiros não nulos e x, y inteiros quaisquer.

(a) Se $b \mid a$ e $a \mid b$, então $a = \pm b$.

(b) Se $c \mid b$ e $b \mid a$, então $c \mid a$.

(c) Se $c \mid a$ e $c \mid b$, então $c \mid (ax + by)$.

(d) Se $b \mid a$, então $|b| \leq |a|$.

(e) Se $c \mid b$, então $c \mid ab$.

(f) Se $b \mid a$, então $bc \mid ac$.

Prova.
(a) Se a' e b' são inteiros tais que $a = ba'$ e $b = ab'$, então $a = (ab')a' = a(a'b')$ e, daí, $a'b' = 1$. Logo, $a' = \pm 1$, donde segue que $a = \pm b$.

(b) Se $a = ba'$ e $b = cb'$, com $a', b' \in \mathbb{Z}$, então $a = (cb')a' = c(a'b')$, com $a'b' \in \mathbb{Z}$. Logo, $c \mid a$.

(c) Sejam $a = ca'$ e $b = cb'$, com $a', b' \in \mathbb{Z}$. Então $ax + by = ca'x + cb'y = c(a'x + b'y)$, com $a'x + b'y \in \mathbb{Z}$. Logo, $c \mid (ax + by)$.

(d) Se $a = ba'$, com $a' \in \mathbb{Z}$, então $a \neq 0 \Rightarrow a' \neq 0$ e, daí, $|a'| \geq 1$. Logo, $|a| = |ba'| = |b||a'| \geq |b|$.

(e) Se $b = cb'$, com $b' \in \mathbb{Z}$, então $ab = c(ab')$, com $ab' \in \mathbb{Z}$. Logo, $c \mid ab$.

(f) Se $a = ba'$, com $a' \in \mathbb{Z}$, então $ac = (bc)a'$ e, daí, $bc \mid ac$. ■

Observações 1.6.

i. Como caso particular do item (c) da proposição anterior, se $c \mid a$ e $c \mid b$, então $c \mid (a \pm b)$. Utilizaremos essa observação várias vezes no que segue.

ii. O item (c) da proposição acima pode ser facilmente generalizado para provar que, se $c \mid a_1, \ldots, a_n$, então $c \mid (a_1x_1 + \cdots + a_nx_n)$, para todos $x_1, \ldots, x_n \in \mathbb{Z}$.

iii. Segue do item (d) acima que todo inteiro não nulo tem somente um número finito de divisores.

Continuando, recorde (cf. problema 1.1.6, volume 3) que, dado $x \in \mathbb{R}$, sua **parte inteira** $\lfloor x \rfloor$ é definida por

$$\lfloor x \rfloor = \max\{n \in \mathbb{Z};\ n \leq x\}. \tag{1.1}$$

De outro modo, para $n \in \mathbb{Z}$, temos

$$\lfloor x \rfloor = n \Leftrightarrow n \leq x < n + 1. \tag{1.2}$$

Por exemplo, como $1 < \sqrt{2} < 2$, temos $\lfloor \sqrt{2} \rfloor = 1$; como $-3 < -2,3 < -2$, temos $\lfloor -2,3 \rfloor = -3$.

A próxima proposição é conhecida como o **algoritmo da divisão** para números inteiros e é um dos pilares da teoria básica de divisibilidade.

Proposição 1.7. Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que $a = bq + r$, com $0 \leq r < |b|$. Ademais, se $b > 0$, então

$$q = \left\lfloor \frac{a}{b} \right\rfloor \quad \text{e} \quad r = a - \left\lfloor \frac{a}{b} \right\rfloor b. \tag{1.3}$$

Tais inteiros q e r são, respectivamente, o **quociente** e o **resto** da divisão de a por b.

Prova. Suponha primeiro $b > 0$, e seja q o maior inteiro tal que $bq \leq a$. Então $bq \leq a < b(q+1)$, de modo que $0 \leq a - bq < b$ e basta definir $r = a - bq$ (observe que, caso $b > 0$, tal inteiro q é precisamente $\lfloor \frac{a}{b} \rfloor$). Se $b < 0$, então $-b > 0$, donde existem $q, r \in \mathbb{Z}$ tais que $a = (-b)q + r$, com $0 \leq r < -b$. Daí, $a = b(-q) + r$, com $0 \leq r < -b = |b|$.

Suponha, agora, que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$ e $0 \leq r, r' < |b|$. Então

$$|r' - r| < |b| \text{ e } b(q - q') = r' - r.$$

Se $q \neq q'$, então $|q - q'| \geq 1$, de modo que

$$|b| \leq |b| \cdot |q - q'| = |r' - r| < |b|,$$

uma contradição. Portanto, $q = q'$ e, daí, $r = r'$. ■

O corolário a seguir, além de importante em si, ilustra em sua prova a utilização típica que fazemos do algoritmo da divisão. Para o enunciado do mesmo, lembre-se de que um inteiro positivo m é dito um **quadrado perfeito** se $m = n^2$, para algum inteiro n (o qual, sempre que conveniente, podemos supor não negativo).

Corolário 1.8. Todo quadrado perfeito:

(a) deixa resto 0 ou 1 quando dividido por 3.

(b) deixa resto 0 ou 1 quando dividido por 4.

(c) deixa resto $0, 1$ ou 4 quando dividido por 8.

Prova. Seja n um natural.

(a) Pelo algoritmo da divisão, o resto da divisão de n por 3 é $0, 1$ ou 2, de modo que $n = 3q$, $3q + 1$ ou $3q + 2$, para algum $q \in \mathbb{Z}$. Agora:

- Se $n = 3q$, então $n^2 = 3 \cdot 3q^2$.
- Se $n = 3q + 1$, então $n^2 = 3(3q^2 + 2q) + 1$.
- Se $n = 3q + 2$, então $n^2 = 3(3q^2 + 4q + 1) + 1$.

No primeiro caso acima, n^2 deixa resto 0 quando dividido por 3; nos outros dois casos, n^2 deixa resto 1 quando dividido por 3.

(b) Novamente pelo algoritmo da divisão, o resto da divisão de n por 4 é $0, 1, 2$ ou 3, de modo que $n = 4q$,$4q+1$, $4q+2$ ou $4q+3$, para algum $q \in \mathbb{Z}$, e podemos dar uma prova análoga à do item (a). Vejamos, contudo, uma prova mais simples: invocando o algoritmo da divisão (ou o exemplo 1.2), temos $n = 2q$ ou $2q + 1$ para algum $q \in \mathbb{Z}$.

- Se $n = 2q$, então $n^2 = 4q^2$.
- Se $n = 2q + 1$, então $n^2 = 4(q^2 + q) + 1$.

No primeiro caso, n^2 deixa resto 0 quando divididido por 4; no segundo, n^2 deixa resto 1 quando dividido por 4.

(c) Uma vez mais, poderíamos apelar diretamente ao algoritmo da divisão, escrevendo $n = 8q + r$ para algum $q \in \mathbb{Z}$ e algum $r \in \{0, 1, 2, \ldots, 7\}$, dando uma prova análoga à do item (a). No entanto, temos pelo item (b) que:

- Se $n = 2q$, então $n^2 = 4q^2$. Há, agora, duas possibilidades:
  - Se q^2 for par, digamos $q^2 = 2k$ para algum $k \in \mathbb{N}$, então $n^2 = 8k$.
  - Se q^2 for ímpar, digamos $q^2 = 2k + 1$ para algum $k \in \mathbb{N}$, então $n^2 = 8k + 4$.

- Se $n = 2q + 1$, então $n^2 = 4q(q + 1) + 1$. Mas, como ao menos um dos inteiros $q, q + 1$ é par, temos $q(q + 1) = 2k$ para algum $k \in \mathbb{N}$, de sorte que $n^2 = 8k + 1$.

Por fim, os casos acima garantem que o resto da divisão de n^2 por 8 só pode ser igual a 0, 1 ou 4. ■

Corolário 1.9. Dados inteiros a_1, a_2 e b, sendo b não nulo, temos que $b \mid (a_1 - a_2)$ se, e só se, a_1 e a_2 deixam restos iguais na divisão por b.

Prova. Suponha primeiro que $a_1 = bq_1 + r$ e $a_2 = bq_2 + r$, com $q_1, q_2, r \in \mathbb{Z}$. Então $a_1 - a_2 = b(q_1 - q_2)$, i.e., $b \mid (a_1 - a_2)$. Reciprocamente, suponha que $b \mid (a_1 - a_2)$, e sejam $a_1 = bq_1 + r_1$, $a_2 = bq_2 + r_2$, com $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ e $0 \leq r_1, r_2 < |b|$. Então

$$a_1 - a_2 = (q_1 - q_2)b + (r_1 - r_2)$$

e, como $b \mid (a_1 - a_2)$ e $b \mid (q_1 - q_2)b$, segue do item (c) da proposição 1.5 que b divide $r_1 - r_2 = (a_1 - a_2) - (q_1 - q_2)b$. Por outro lado, $0 \leq r_1, r_2 < |b|$ implica $|r_1 - r_2| < |b|$, de modo que a única possibilidade é ser $|r_1 - r_2| = 0$ ou, ainda, $r_1 = r_2$. ■

Como aplicação do corolário acima, calculamos a seguir os possíveis valores do último algarismo de um quadrado perfeito.

Exemplo 1.10. O último algarismo de um quadrado perfeito só pode ser $0, 1, 4, 5, 6$ ou 9.

Prova. Observe primeiro que o resto da divisão de um número natural por 10 coincide com seu último algarismo (o algarismo mais à direita, na representação decimal do número). De fato, seja $m = 10m' + a_0$, com $m' \in \mathbb{Z}_+$ e $0 \leq a_0 \leq 9$; como o inteiro $10m'$ termina por 0, segue que a representação decimal da soma $10m' + a_0$ (que é igual a m) termina à direita com o algarismo a_0.

Sejam, agora, $n \in \mathbb{N}$ e $q, r \in \mathbb{Z}$ tais que $n = 10q + r$, com $0 \leq r \leq 9$. Então

$$\begin{aligned} n^2 &= (10q + r)^2 = 100q^2 + 20qr + r^2 \\ &= 10(10k^2 + 2kr) + r^2, \end{aligned}$$

de sorte que $10 \mid (n^2 - r^2)$ e o corolário 1.9 garante que n^2 e r^2 deixam restos iguais na divisão por 10. Portanto, segue de nossa observação inicial que o último algarismo de n^2 é igual ao último algarismo de r^2.

Para terminar, basta checar quais são os últimos algarismos dos números r^2 quando r varia de 0 a 9: $0^2 = 0$; 1^2 e 9^2 terminam em 1; 2^2 e 8^2 terminam em 4; 3^2 e 7^2 terminam em 9; 4^2 e 6^2 terminam em 6; 5^2 termina em 5. Assim, os possíveis últimos algarismos de n^2 são 0, 1, 4, 5, 6 ou 9. ■

Exemplo 1.11. Seja $n > 1$ inteiro. Mostre que qualquer sequência de n inteiros consecutivos possui exatamente um múltiplo de n.

Prova. Seja $a + 1, a + 2, \ldots, a + n$ uma sequência de n inteiros consecutivos, com $a = nq + r$, $0 \leq r < n$. Então $0 < n - r \leq n$, de modo que $a + (n - r)$ é um dos números de nossa sequência. Mas

$$a + (n - r) = (nq + r) + (n - r) = n(q + 1),$$

um múltiplo de n.

Para o que falta, usemos novamente o corolário 1.9: os números $a + 1, a + 2, \ldots, a + n$ deixam restos dois a dois distintos na divisão por n, uma vez que o módulo da diferença de dois quaisquer deles é no mínimo 1 e no máximo $n - 1$. Logo, há no máximo um múltiplo de n em nossa sequência. ■

Problemas – Seção 1.1

1. Prove o **critério de divisibilidade** por 9: o resto da divisão de um número natural por 9 é igual ao resto da divisão por 9 da soma dos algarismos de sua representação decimal. Em particular, um natural é múltiplo de 9 se, e só se, a soma de seus algarismos o for.

2. Encontre o resto da divisão do número 10^k por 11.

3. Prove o **critério de divisibilidade** por 11: se o número natural n tem representação decimal $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$, então o resto da divisão de n por 11 é igual ao resto da divisão por 11 da *soma alternada*

$$a_0 - a_1 + a_2 - \ldots + (-1)^{k-1} a_{k-1} + (-1)^k a_k.$$

Em particular, $11 \mid n$ se, e só se, 11 dividir a soma alternada dos algarismos de n.

4. (IMO.) Encontre todos os naturais n de três algarismos, tais que $11 \mid n$ e $\frac{n}{11}$ é igual à soma dos quadrados dos algarismos de n.

5. (IMO.) Ache todos os $n \in \mathbb{N}$ tais que o produto dos algarismos da representação decimal de n seja igual a $n^2 - 10n - 22$.

6. * Dado um natural n, prove que o produto de n inteiros consecutivos é sempre divisível por $n!$.

7. (Hungria.) Para $n \in \mathbb{N}$, prove que o número $8^n - 3^n - 6^n + 1^n$ é um múltiplo de 10.

8. (Hungria.) Prove que 5 divide $1^{99} + 2^{99} + 3^{99} + 4^{99} + 5^{99}$.

Para o próximo problema, dado $m \in \mathbb{Z}$, denotemos por $\mathbb{Z}m$ o conjunto

$$\mathbb{Z}m = \{mq;\ q \in \mathbb{Z}\} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

9. Seja S um conjunto de números inteiros, contendo 0 e satisfazendo a seguinte propriedade:

$$x, y \in S,\ x \neq y \Rightarrow x - y \in S.$$

Se $S \neq \{0\}$, prove que:

(a) $S \cap \mathbb{N} \neq \emptyset$.

(b) Se $x, y \in S$, então $x + y \in S$.

(c) Se $m = \min(S \cap \mathbb{N})$, então $S = \mathbb{Z}m$.

10. * Calcule o resto da divisão de $2^{64} + 1$ por $2^{32} + 1$. Mais geralmente, dados a, m e n inteiros maiores que 1 e tais que $m > n$, calcule o resto da divisão de $a^{2^m} + 1$ por $a^{2^n} + 1$.

11. * Para $x \in \mathbb{R}$, prove os seguintes itens:

(a) $x - 1 < \lfloor x \rfloor \leq x$.

(b) $\lfloor x + 1 \rfloor = \lfloor x \rfloor + 1$.

(c) $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0, & \text{se } x \in \mathbb{Z} \\ -1, & \text{se } x \notin \mathbb{Z} \end{cases}$.

12. * Sejam $x, y \in \mathbb{R}$ e m, n inteiros quaisquer, sendo $n > 0$. Prove os seguintes itens:

(a) $x \leq y \Rightarrow \lfloor x \rfloor \leq \lfloor y \rfloor$.

(b) $\lfloor nx \rfloor \geq n \lfloor x \rfloor$.

(c) $\left\lfloor \frac{m+1}{n} \right\rfloor \leq \left\lfloor \frac{m}{n} \right\rfloor + 1$.

(d) $\left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor = \left\lfloor \frac{x}{n} \right\rfloor$.

(e) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.

(f) $\lfloor x+y \rfloor + \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor$.

13. Para $x \in \mathbb{R}$, prove que o **inteiro mais próximo** de x é o inteiro $\lfloor x + \frac{1}{2} \rfloor$.

14. (ORM.) Encontre todos os $a, b \in \mathbb{N}$ tais que

$$\left\lfloor \frac{a^2}{b} \right\rfloor + \left\lfloor \frac{b^2}{a} \right\rfloor + 1 = \left\lfloor \frac{a^2+b^2}{ab} \right\rfloor + ab.$$

15. Prove que não existem inteiros ímpares x, y e z tais que

$$(x+y)^2 + (y+z)^2 = (x+z)^2.$$

16. Sejam x, y e z inteiros tais que $x^2 + y^2 = z^2$. Prove que $6 \mid xy$.

Para o problema a seguir, lembre-se de que um **cubo perfeito** é um inteiro da forma q^3, para algum $q \in \mathbb{Z}$.

17. (OBM - adaptado.)

(a) Encontre os possíveis restos da divisão de um cubo perfeito por 7.

(b) Se x, y, z são inteiros tais que $x^3 + y^3 - z^3$ é múltiplo de 7, prove que ao menos um dentre os números x, y, z é múltiplo de 7.

18. (OBM.) Ache todos os x, y, z, n naturais tais que $n^x + n^y = n^z$.

19. (União Soviética.) Para $n > 3$ inteiro, mostre que o número $1! + 2! + 3! + \cdots + n!$ nunca é um quadrado perfeito.

20. (OBM.) Prove que não existem inteiros x e y tais que $15x^2 - 7y^2 = 9$.

21. (França.) Para $k, m, n \in \mathbb{N}$, com $k > 2$, sejam $F_m = 2^{2^m} + 1$ o $m-$ésimo **número de Fermat** e $G_n = \frac{n(n-1)}{2}(k-2) + n$. Fixado k, queremos encontrar (se existirem) os $m, n \in \mathbb{N}$ tais que $F_m = G_n$. Para tanto, faça os seguintes itens:

(a) Prove que, se existir um tal par (m, n), então há um inteiro não negativo r tal que $n = 2^r + 1$.

(b) Conclua, a partir de (a), que $k - 1 = 2^r t_1$, para algum $t_1 \in \mathbb{N}$, de sorte que $2^{2^m} + 1 = 2^{2r}(2^r t_1 + t_1 - 1)$.

(c) Mostre, por indução sobre o natural l, que se tivermos $2^{2^m} + 1 = 2^{(l+1)r}(2^r t_l + t_l \mp 1)$, para algum $t_l \in \mathbb{N}$, então $2^{2^m} + 1 = 2^{(l+2)r}(2^r t_{l+1} + t_{l+1} \pm 1)$.

(d) Conclua sobre a existência de tais pares (m, n).

1.2 MDC e MMC

Se $a_1, \ldots, a_n$ são inteiros não nulos dados, dizemos que um inteiro d é um **divisor comum** de $a_1, \ldots, a_n$ quando $d \mid a_1, \ldots, d \mid a_n$. Note que $a_1, \ldots, a_n$ sempre têm divisores comuns: 1, por exemplo. Ademais, desde que qualquer inteiro não nulo tem apenas um número finito de divisores, $a_1, \ldots, a_n$ têm apenas um número finito de divisores comuns. Assim, a definição a seguir tem sentido.

Definição 1.12. O **máximo divisor comum** dos inteiros não nulos $a_1, a_2, \ldots, a_n$, denotado $\mathrm{mdc}\,(a_1, a_2, \ldots, a_n)$, é o maior dentre os divisores comuns de $a_1, a_2, \ldots, a_n$. Os inteiros $a_1, a_2, \ldots, a_n$ são **primos entre si**, ou **relativamente primos**, se $\mathrm{mdc}\,(a_1, a_2, \ldots, a_n) = 1$.

Para o teorema a seguir, devido ao matemático francês Étienne Bézout, dado $n \in \mathbb{Z}$ denote por $n\mathbb{Z}$ o conjunto dos múltiplos inteiros de n, i.e.,

$$n\mathbb{Z} = \{nx;\ x \in \mathbb{Z}\} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}.$$

Figura 1.1: Étienne Bézout, matemático francês do século XVIII, um dos precursores da área da Matemática hoje conhecida como Geometria Algébrica. Em que pese seu teorema sobre o mdc, o mais famoso teorema de Bézout é provavelmente aquele que afirma que, sendo f e g polinômios reais em X e Y, sem fatores comuns e de graus respectivamente m e n, o número de pontos de interseção das *curvas* $f(x,y) = 0$ e $g(x,y) = 0$ no plano Cartesiano é no máximo mn. Para uma exposição elementar, sugerimos [11].

Teorema 1.13 (Bézout). Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos dados. Se

$$S = \{\sum_{i=1}^{n} a_i x_i;\ x_i \in \mathbb{Z},\ \forall\, 1 \le i \le n\},$$

então $S = d\mathbb{Z}$, onde $d = \text{mdc}\,(a_1, a_2, \ldots, a_n)$. Em particular, existem números inteiros $u_1, \ldots, u_n$ tais que

$$\text{mdc}\,(a_1, a_2, \ldots, a_n) = a_1u_1 + a_2u_2 + \cdots + a_nu_n. \tag{1.4}$$

Prova. É imediato que todo múltiplo de um elemento de S pertence a S. Por outro lado, como d divide $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ para todos $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, temos que $S \subset d\mathbb{Z}$.

Para estabelecer a inclusão contrária, note primeiro que S contém inteiros positivos; de fato, escolhendo $x_1 = a_1$ e $x_2 = \cdots = x_n = 0$, por exemplo, concluímos que

$$a_1^2 = a_1x_1 + a_2x_2 + \cdots + a_nx_n \in S.$$

Como S contém inteiros positivos, existe um menor inteiro positivo d' em S. Se mostrarmos que $d' = d$, seguirá que $d \in S$ e nossa observação inicial garantirá que $d\mathbb{Z} \subset S$.

Afirmamos, inicialmente, que $d' \mid a_1, \ldots, a_n$. De fato, como $d' \in S$, existem $u_1, u_2, \ldots, u_n \in \mathbb{Z}$ tais que $d' = a_1u_1 + a_2u_2 + \cdots + a_nu_n$. Agora, seja $a_1 = d'q + r$, com $q, r \in \mathbb{Z}$ e $0 \le r < d'$. Então

$$\begin{aligned} r &= a_1 - d'q \\ &= a_1 - (a_1u_1 + a_2u_2 + \cdots + a_nu_n)q \\ &= a_1(1 - u_1q) + a_2(-u_2q) + \cdots + a_n(-u_nq), \end{aligned}$$

de sorte que $r \in S$. Se $0 < r < d'$, teríamos uma contradição ao fato de ser d' o menor inteiro positivo pertencente a S. Logo, $r = 0$ e $d' \mid a_1$. Analogamente, $d' \mid a_2, \ldots, a_n$.

Para terminar, como d' é um divisor comum de $a_1, a_2, \ldots, a_n$, para mostrarmos que $d' = d$ basta que seja $d' \ge d$. Mas, se $a_1 = dq_1$, $a_2 = dq_2$, $\ldots$, $a_n = dq_n$, com $q_1, q_2, \ldots, q_n \in \mathbb{Z}$, então

$$\begin{aligned} d' &= a_1u_1 + a_2u_2 + \cdots + a_nu_n \\ &= dq_1u_1 + dq_2u_2 + \cdots + dq_nu_n \\ &= d(q_1u_1 + q_2u_2 + \cdots + q_nu_n), \end{aligned}$$

ou seja, $0 < d \mid d'$. Logo, $d \le d'$. ■

Colecionamos, a seguir, vários corolários úteis do teorema acima.

Corolário 1.14. Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos e d seu mdc. Se $d' \in \mathbb{N}$, então $d' \mid a_1, a_2, \ldots, a_n$ se, e só se, $d' \mid d$.

Prova. Tome inteiros $u_1, u_2, \ldots, u_n$ tais que $d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$. Uma vez que $d' \mid a_1, a_2, \ldots, a_n$, o item i. das observações 1.6 garante que $d' \mid d$. A recíproca é imediata. ■

Corolário 1.15. Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos dados e d seu mdc.

(a) $d = 1$ se, e só se, existirem inteiros $u_1, u_2, \ldots, u_n$ tais que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = 1$.

(b) $\text{mdc}\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1$.

Prova.
(a) Se $d = 1$, a existência de inteiros $u_1, u_2, \ldots, u_n$ como pede o enunciado segue do teorema de Bézout. Reciprocamente, sejam $u_1, u_2, \ldots, u_n$ inteiros como no enunciado. Como $d \mid a_1, a_2, \ldots, a_n$, segue novamente do item i. das observações 1.6 que $d \mid (a_1u_1 + \cdots + a_nu_n)$, i.e., $d \mid 1$. Logo, $d = 1$.

(b) Sendo $d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$, temos $\left(\frac{a_1}{d}\right)u_1 + \cdots + \left(\frac{a_n}{d}\right)u_n = 1$, e o resultado segue imediatamente do item (a). ■

Exemplo 1.16 (China). Sejam a, b, c, d inteiros não nulos, tais que $c + d \neq 0$ e $ad - bc = 1$. Prove que a fração $\dfrac{a+b}{c+d}$ é irredutível.

Prova. Queremos provar que $\text{mdc}\,(a + b, c + d) = 1$. Para tanto, procuremos, de acordo com o corolário acima, inteiros u, v tais que

$$(a + b)u + (c + d)v = 1.$$

Ora, uma vez que $ad - bc = 1$, basta tomarmos $u = d$ e $v = -b$. ■

Observação 1.17. Se $a_1, a_2, \ldots, a_n$ são inteiros não nulos com mdc igual a d, o item (b) do corolário anterior garante que, fazendo $u_i = \frac{a_i}{d}$ para $1 \leq i \leq n$, temos $u_1, u_2, \ldots, u_n$ primos entre si e $a_1 = du_1$, $a_2 = du_2$, ..., $a_n = du_n$.

A forma de escrever inteiros não nulos $a_1, a_2, \ldots, a_n$, como descrito na observação acima, é útil na análise de várias situações, como atestam os exemplos a seguir.

Exemplo 1.18. Todo racional não nulo admite uma representação em **fração irredutível**, i.e., uma fração da forma $\frac{a}{b}$, com a e b inteiros não nulos e primos entre si. De fato, seja r um racional não nulo e $r = \frac{m}{n}$ uma representação fracionária de r. Então, m e n são inteiros não nulos e, sendo $d = \text{mdc}\,(m, n)$, $m = da$ e $n = db$, segue do item (b) do corolário 1.15 que $\text{mdc}\,(a, b) = 1$. Por outro lado,

$$r = \frac{m}{n} = \frac{da}{db} = \frac{a}{b},$$

o que nos dá a representação desejada de r em fração irredutível.

Exemplo 1.19 (Rússia). Sejam a, b naturais tais que $\frac{a+1}{b} + \frac{b+1}{a} \in \mathbb{N}$. Prove que

$$\text{mdc}\,(a, b) \leq \sqrt{a + b}.$$

Prova. Sendo $d = \text{mdc}\,(a, b)$, existem inteiros u, v tais que $a = du$, $b = dv$ e $\text{mdc}\,(u, v) = 1$. Então

$$\begin{aligned} \frac{a+1}{b} + \frac{b+1}{a} &= \frac{du+1}{dv} + \frac{dv+1}{du} \\ &= \frac{u(du+1) + v(dv+1)}{duv} \\ &= \frac{d(u^2+v^2) + (u+v)}{duv} \in \mathbb{N}, \end{aligned}$$

de modo que

$$uv \cdot \frac{d(u^2+v^2) + (u+v)}{duv} = (u^2 + v^2) + \frac{u+v}{d}$$

também é natural. Portanto, $d \mid (u+v)$ e, daí, $d \leq u+v$. Mas isso é o mesmo que

$$d^2 \leq du + dv = a + b.$$

■

Corolário 1.20. Para $a_1, \ldots, a_n, k$ inteiros não nulos, temos:

(a) $\text{mdc}\,(ka_1, \ldots, ka_n) = |k|\,\text{mdc}\,(a_1, \ldots, a_n)$.

(b) $\text{mdc}\,(a_1, \ldots, a_n) = \text{mdc}\,(\,\text{mdc}\,(a_1, \ldots, a_{n-1}), a_n)$.

Prova.
(a) Denotemos $d = \text{mdc}\,(a_1, \ldots, a_n)$ e $d' = \text{mdc}\,(ka_1, \ldots, ka_n)$. Como $d \mid a_1, \ldots, a_n$, temos que $|k|d \mid ka_1, \ldots, ka_n$, i.e., $|k|d$ é um divisor comum positivo de $ka_1, \ldots, ka_n$. Mas, como d' é o maior dentre tais divisores comuns, segue que $|k|d \leq d'$. Reciprocamente, como k divide d' e d' divide $ka_1, \ldots, ka_n$, temos que $\frac{d'}{|k|}$ é um inteiro positivo que divide $a_1, \ldots, a_n$, de maneira que $\frac{d'}{|k|} \leq d$ ou, o que é o mesmo, $d' \leq |k|d$. Logo, $d' = |k|d$.

(b) Exercício.

■

Especializemos nossa discussão ao máximo divisor comum de dois inteiros não nulos. Dados a, b inteiros não nulos, com $d = \text{mdc}\,(a,b)$, o teorema de Bézout garante a existência de inteiros u e v tais que $d = au + bv$. É importante notar que tal maneira de escrever o mdc não é única; de fato, se $t \in \mathbb{Z}$, então temos também $d = a(u - tb) + b(v + ta)$ (teremos mais a dizer sobre isso na proposição 1.25).

Mais adiante, estabeleceremos um algoritmo muito útil e importante para encontrar efetivamente o mdc de dois inteiros, o *algoritmo de Euclides*. Comecemos estudando algumas propriedades do mdc de dois inteiros não nulos.

Proposição 1.21. Para a, b e c inteiros não nulos, temos que:

(a) Se $c \mid ab$ e $\text{mdc}\,(b,c) = 1$, então $c \mid a$.

(b) Se $a + bc \neq 0$, então $\text{mdc}\,(a+bc, b) = \text{mdc}\,(a,b)$.

(c) Se $\text{mdc}\,(a,c) = 1$, então $\text{mdc}\,(a, bc) = \text{mdc}\,(a,b)$.

(d) Se $c \mid b$ e $\text{mdc}\,(a,b) = 1$, então $\text{mdc}\,(a,c) = 1$.

(e) Se $\text{mdc}\,(b,c) = 1$, então $\text{mdc}\,(a, bc) = \text{mdc}\,(a,b)\,\text{mdc}\,(a,c)$. Em particular, se b e c são primos entre si e dividem a, então bc divide a.

Prova.
(a) Sejam u, v inteiros tais que $bu + cv = 1$. Multiplicando ambos os membros dessa igualdade por a, obtemos $(ab)u + c(av) = a$. Por fim, como $c \mid (ab)$, segue do item (c) da proposição 1.5 que $c \mid a$.

(b) Sejam $d = \text{mdc}\,(a+bc, b)$ e $d' = \text{mdc}\,(a,b)$. Como $d' \mid a, b$, temos que $d' \mid a, a+bc$. Portanto, pelo corolário 1.14 temos que $d' \mid d$. Reciprocamente, como $d \mid (a+bc)$ e $d \mid b$, temos que $d \mid [(a+bc) - bc]$, i.e., $d \mid a$ e $d \mid b$. Novamente pelo corolário 1.14, temos que $d \mid d'$ e, assim, $d = d'$.

(c) Sejam $d = \text{mdc}\,(a,b)$ e $d' = \text{mdc}\,(a,bc)$. De $d \mid b$, segue que $d \mid bc$. Assim, $d \mid a$ e $d \mid bc$, de sorte que $d \mid \text{mdc}\,(a,bc) = d'$. Para terminar, mostremos que $d' \mid d$: como $\text{mdc}\,(a,c) = 1$, segue do teorema de Bézout a existência de $u, v \in \mathbb{Z}$ tais que $au + cv = 1$ e, daí, $a(bu) + (bc)v = b$; mas, como $d' \mid a$ e $d' \mid bc$, temos que $d' \mid b$. Então, $d' \mid a$ e $d' \mid b$, de modo que $d' \mid \text{mdc}\,(a,b) = d$.

(d) Sejam $d \in \mathbb{Z}$ tal que $b = cd$ e $u, v \in \mathbb{Z}$ tais que $au + bv = 1$. Então, $au + c(dv) = 1$ e segue, do item (a) do corolário 1.15, que

$\text{mdc}\,(a,c) = 1$.

(e) Sejam $d = \text{mdc}\,(a,b)$ e $a = du$, $b = dv$, com u e v inteiros primos entre si. Aplicando sucessivamente o corolário 1.22 e o item (c), obtemos

$$\text{mdc}\,(a,bc) = \text{mdc}\,(du,dvc) = d\,\text{mdc}\,(u,vc) = d\,\text{mdc}\,(u,c).$$

Mas, $d \mid b$ e $\text{mdc}\,(b,c) = 1$ implicam (cf. item (d)) $\text{mdc}\,(d,c) = 1$. Portanto, mais uma aplicação do item (c) nos dá

$$\text{mdc}\,(a,c) = \text{mdc}\,(du,c) = \text{mdc}\,(u,c).$$

Finalmente, juntando as duas relações acima, obtemos

$$\text{mdc}\,(a,bc) = d \cdot \text{mdc}\,(u,c) = \text{mdc}\,(a,b)\,\text{mdc}\,(a,c).$$

O resto é imediato. ■

Corolário 1.22. Sejam a e b inteiros não nulos e k, m e n números naturais.

(a) Se $\text{mdc}\,(a,b) = 1$, então $\text{mdc}\,(a^m,b^n) = 1$.

(b) Se $\text{mdc}\,(a,b) = 1$ e $ab = k^n$, então existem $u,v \in \mathbb{Z}$ tais que $a = u^n$, $b = v^n$.

Prova.
(a) Aplicando o item (c) da proposição anterior, com b^{n-1} no lugar de b e b no lugar de c, obtemos

$$\text{mdc}\,(a,b^n) = \text{mdc}\,(a,b^{n-1}\cdot b) = \text{mdc}\,(a,b^{n-1}).$$

Segue por indução sobre n que $\text{mdc}\,(a,b^n) = \text{mdc}\,(a,b) = 1$. Analogamente,

$$\text{mdc}\,(a^m,b^n) = \text{mdc}\,(a^{m-1}\cdot a,b^n) = \text{mdc}\,(a^{m-1},b^n)$$

e, por indução sobre m, obtemos $\text{mdc}\,(a^m,b^n) = \text{mdc}\,(a,b^n) = 1$.

Alternativamente, uma vez que $\text{mdc}\,(a,b) = 1$, o teorema de Bézout garante a existência de $x,y \in \mathbb{Z}$ tais que $ax + by = 1$. Portanto, segue da fórmula de expansão binomial que

$$1 = (ax+by)^n = \sum_{k=0}^{n-1} \binom{n}{k} (ax)^{n-k}(by)^k + (by)^n = aq + b^n y^n,$$

onde $q = \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k-1} x^{n-k} (by)^k$. Portanto, segue do item (a) do corolário 1.15 que $\text{mdc}\,(a,b^n) = 1$. Argumentando de maneira análoga, concluímos que $\text{mdc}\,(a^m,b^n) = 1$.

(b) Sejam $u = \text{mdc}\,(a,k)$ e $v = \text{mdc}\,(b,k)$. Como $\text{mdc}\,(a,b) = 1$, o item (d) da proposição anterior garante que

$$k = \text{mdc}\,(k^n,k) = \text{mdc}\,(ab,k) = \text{mdc}\,(a,k)\cdot\text{mdc}\,(b,k) = uv,$$

de modo que

$$ab = k^n = u^n v^n.$$

Agora, $u \mid a$ e $\text{mdc}\,(a,b) = 1$ nos dão (cf. item (d) da proposição anterior) $\text{mdc}\,(u,b) = 1$; analogamente, $\text{mdc}\,(v,a) = 1$. Segue, pois, do item (a) que

$$\text{mdc}\,(u^n,b) = 1 \quad \text{e} \quad \text{mdc}\,(v^n,a) = 1.$$

Por fim,

$$\begin{cases} u^n \mid ab \ \text{ e } \ \text{mdc}\,(u^n,b) = 1 \Rightarrow u^n \mid a \Rightarrow u^n \leq a \\ v^n \mid ab \ \text{ e } \ \text{mdc}\,(v^n,a) = 1 \Rightarrow v^n \mid b \Rightarrow v^n \leq b \end{cases}.$$

Mas, como $ab = u^n v^n$, $u^n \leq a$ e $v^n \leq b$, a única possibilidade é que sejam $a = u^n$ e $b = v^n$. ■

Exemplo 1.23. Dados números naturais n e k, com $k > 1$, ou existe $m \in \mathbb{N}$ tal que $n = m^k$ ou $\sqrt[k]{n}$ é um número irracional.

Prova. Se $\sqrt[k]{n} = \frac{m}{p}$, com m e p naturais primos entre si (cf. exemplo 1.18), então $p^k n = m^k$. Mas, como $\text{mdc}\,(m, p) = 1$, segue do corolário acima que $\text{mdc}\,(m^k, p^k) = 1$. Por outro lado, $p^k n = m^k$ garante que $p^k \mid m^k$. Assim, a única maneira de p^k e m^k serem relativamente primos é que seja $p^k = 1$. Mas, como $k > 1$, devemos ter, então, $p = 1$, i.e., $n = m^k$. ■

Uma equação em números inteiros e com mais de uma variável é denominada uma **equação Diofantina**, em homenagem ao matemático grego Diofanto de Alexandria[1], quem primeiro tentou estudar sistematicamente as soluções de algumas dessas equações. A análise de equações Diofantinas gerais é uma tarefa das mais difíceis, exigindo em geral argumentos bastante sofisticados. Vejamos um exemplo simples.

Exemplo 1.24. Prove que não existem $x, y \in \mathbb{N}$ tais que $x^3 + 3 = 4y(y + 1)$.

Prova. Suponha o contrário, i.e., que $x^3 + 3 = 4y(y + 1)$, para certos $x, y \in \mathbb{N}$. Então

$$x^3 + 4 = 4y(y + 1) + 1 = (2y + 1)^2$$

e, daí,

$$x^3 = (2y + 1)^2 - 2^2 = (2y - 1)(2y + 3).$$

Agora, se $d = \text{mdc}\,(2y - 1, 2y + 3)$, então d é ímpar e divide $(2y + 3) - (2y - 1) = 4$, de maneira que $d = 1$. Portanto, o produto dos inteiros primos entre si $2y - 1$ e $2y + 3$ é um cubo perfeito, e o corolário 1.22 garante que ambos $2y - 1$ e $2y + 3$ devem ser cubos perfeitos. Mas, como

[1]Matemático grego do século III d.C., considerado um dos *pais* da Álgebra e da Teoria dos Números. Em seu livro *Aritmética*, Diofanto procurou, pela primeira vez, estudar sistematicamente as soluções inteiras de certos tipos particulares de equações polinomiais – de fato, essa nomenclatura não estava disponível à sua época –, as quais passaram, merecidamente, a ser conhecidas como *Diofantinas*.

não há dois cubos perfeitos cuja diferença seja igual a 4, chegamos a uma contradição. ■

Em que pese o caráter *ad hoc* do exemplo acima, a teoria desenvolvida até agora para o estudo do mdc de dois inteiros permite resolver completamente a **equação diofantina linear** a duas variáveis $ax + by = c$, onde x e y são incógnitas inteiras e a, b e c parâmetros inteiros não nulos dados, conforme ensina o resultado a seguir.

Proposição 1.25. Sejam a, b e c inteiros não nulos dados. A equação $ax + by = c$ admite soluções $x, y \in \mathbb{Z}$ se, e só se, $\text{mdc}\,(a, b) \mid c$. Nesse caso, se $d = \text{mdc}\,(a, b)$ e $x = x_0$, $y = y_0$ for uma solução inteira qualquer da equação, então as fórmulas

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \tag{1.5}$$

$t \in \mathbb{Z}$, dão todas as soluções inteiras possíveis. Em particular, podemos supor que seja $x > 0 > y$ ou, ainda, $x < 0 < y$.

Prova. Suponha, inicialmente, que existam inteiros x e y tais que $ax + by = c$. Como $d \mid a$ e $d \mid b$, segue que $d \mid (ax + by)$, ou seja, $d \mid c$. Reciprocamente, seja $c = de$, com $e \in \mathbb{Z}$, e (pelo teorema de Bézout) u e v inteiros tais que $d = au + bv$. Então $c = a \cdot eu + b \cdot ev$, quer dizer, a equação admite a solução inteira $x_0 = eu$, $y_0 = ev$.

Para o que falta, suponha que $d \mid c$ e seja $x = x_0$, $y = y_0$ uma solução inteira qualquer da equação. Se $x = x_1$, $y = y_1$ for outra solução inteira da mesma, teremos $a(x_1 - x_0) = b(y_0 - y_1)$; cancelando d em ambos os membros dessa igualdade, segue que

$$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1).$$

Assim, $\frac{b}{d} \mid \frac{a}{d}(x_1 - x_0)$ e, como $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, o item (a) da proposição anterior garante que $\frac{b}{d} \mid (x_1 - x_0)$. Sendo $x_1 - x_0 = \frac{b}{d}t$, obtemos $y_0 - y_1 = \frac{a}{d}t$ e as fórmulas do enunciado seguem. Reciprocamente, é

imediato verificar que tais fórmulas dão, de fato, soluções inteiras para a equação.

Para o que falta, suponha que $a, b > 0$ (os demais casos podem ser analisados de modo análogo). Como

$$u - tb > 0 \Leftrightarrow t < \frac{u}{b} \text{ e } v + ta < 0 \Leftrightarrow t < -\frac{v}{a},$$

escolhendo um inteiro t tal que $t < \frac{u}{b}, -\frac{v}{a}$ e fazendo $u_1 = u - tb$ e $v_1 = v + ta$, teremos $u_1 > 0$, $v_1 < 0$ e $d = au_1 + bv_1$. Analogamente, mostramos que podemos tomar uma solução $x < 0 < y$ da equação dada. ■

Por enquanto, sabemos apenas que é possível escrever o mdc de dois inteiros não nulos a e b da forma $au + bv$, para algum par de inteiros u, v, sem termos ainda uma maneira razoável para fazer isso efetivamente. Para remediar essa situação, consideremos o seguinte algoritmo, usualmente atribuído a Euclides.

Algoritmo de Euclides

$$\begin{array}{llcll}
\text{Passo } 1 & : a & = & bq_1 + r_1 & 0 < r_1 < b \\
\text{Passo } 2 & : b & = & r_1q_2 + r_2 & 0 < r_2 < r_1 \\
\text{Passo } 3 & : r_1 & = & r_2q_3 + r_3 & 0 < r_3 < r_2 \\
 & & \cdots & & \cdots \\
\text{Passo } j & : r_{j-2} & = & r_{j-1}q_j + r_j & 0 < r_j < r_{j-1} \\
\text{Passo } j+1 & : r_{j-1} & = & r_jq_{j+1} + 0 &
\end{array}$$

Note que a execução do algoritmo realmente para após um número finito de passos, pois, desde que $r_1, r_2, \ldots$ são inteiros para os quais $b > r_1 > r_2 > \cdots \geq 0$, deve existir um menor natural j tal que r_j é o último resto não nulo no processo de divisões acima.

A importância do algoritmo de Euclides é explicada pela proposição a seguir.

Proposição 1.26. Nas notações da tabela acima para o algorimo de Euclides, temos $\text{mdc}\,(a, b) = r_j$.

Prova. Pelo item (b) da proposição 1.21, temos sucessivamente

$$\begin{aligned}
\text{mdc}\,(a, b) &= \text{mdc}\,(a - bq_1, b) = \text{mdc}\,(r_1, b) \\
&= \text{mdc}\,(r_1, b - r_1q_2) = \text{mdc}\,(r_1, r_2) \\
&= \text{mdc}\,(r_1 - r_2q_3, r_2) = \text{mdc}\,(r_3, r_2) \\
&\cdots \\
&= \text{mdc}\,(r_{j-1}, r_j) = r_j,
\end{aligned}$$

onde utilizamos, na última igualdade, o fato de que $r_j \mid r_{j-1}$. ■

Embutido no algoritmo de Euclides também está um método para encontrarmos os inteiros u, v cuja existência é garantida pelo teorema de Bézout, i.e., tais que $\text{mdc}\,(a, b) = au + bv$. Vejamos como proceder através de um exemplo numérico.

Exemplo 1.27. Utilize o algoritmo de Euclides para mostrar que o mdc de 120 e 84 é igual a 12. Em seguida, resolva a equação $120x + 84y = 12$ no conjunto dos inteiros.

Solução. Comecemos executando o algoritmo de Euclides:

$$\begin{aligned}
120 &= 84 \cdot 1 + 36 \\
84 &= 36 \cdot 2 + 12 \\
36 &= 12 \cdot 3.
\end{aligned}$$

Como 12 é o último resto não nulo, segue da proposição 1.26 que

$$\text{mdc}\,(120, 84) = 12.$$

Podemos, agora, encontrar inteiros u e v tais que $12 = 120u + 84v$ trabalhando *de trás para frente* com as divisões sucessivas que nos

levaram ao mdc:

$$\begin{aligned} 12 &= 84\cdot 1 - 36\cdot 2 \\ &= 84\cdot 1 - (120 - 84\cdot 1)\cdot 2 \\ &= 84\cdot 1 - 120\cdot 2 + 84\cdot 2 \\ &= 84\cdot 3 + 120(-2). \end{aligned}$$

Por fim, de posse da solução $x_0 = -2$ e $y_0 = 3$ da equação $120x + 84y = 12$, podemos obter todas as soluções dessa equação utilizando as fórmulas (1.5):

$$\begin{cases} x = & -2 + (84/12)t &= -2 + 7t \\ y = & 3 - (120/12)t &= 3 - 10t \end{cases}.$$

■

O algoritmo de Euclides e sua prova também são úteis para muitos propósitos teóricos, conforme atesta o próximo exemplo.

Exemplo 1.28. Se a, m e n são naturais tais que $a > 1$ e $m = nq + r$, com $0 \leq r < n$, prove que

$$\text{mdc}\,(a^m - 1, a^n - 1) = a^{\text{mdc}\,(m,n)} - 1.$$

Prova. Mostremos inicialmente que, se $r = 0$, então $(a^n - 1) \mid (a^m - 1)$. Para tanto, basta observar que $a^m - 1 = (a^n)^q - 1$ e lembrar que já sabemos, pelo exemplo 1.3, que $a^n - 1$ divide $(a^n)^q - 1$.

Provemos agora que, se $r > 0$, então $\text{mdc}\,(a^m - 1, a^n - 1) = \text{mdc}\,(a^n - 1, a^r - 1)$. De fato, fazendo $a^n = b$ quando conveniente, temos

$$\begin{aligned} a^m - 1 &= a^{nq+r} - 1 = (a^{nq} - 1)a^r + (a^r - 1) \\ &= ((a^n)^q - 1)a^r + (a^r - 1) \\ &= (a^n - 1)(b^{q-1} + \cdots + b + 1)a^r + (a^r - 1). \end{aligned}$$

Sendo

$$\begin{cases} c &= (b^{q-1} + b^{q-2} + \cdots + b + 1)a^r \\ d &= \text{mdc}\,(a^m - 1, a^n - 1) \\ d' &= \text{mdc}\,(a^n - 1, a^r - 1) \end{cases},$$

temos

$$a^m - 1 = (a^n - 1)c + (a^r - 1).$$

Portanto, segue do item (b) da proposição 1.21 que

$$\begin{aligned} \text{mdc}\,(a^m - 1, a^n - 1) &= \text{mdc}\,((a^n - 1)c + (a^r - 1), a^n - 1) \\ &= \text{mdc}\,(a^r - 1, a^n - 1). \end{aligned}$$

Para o que falta suponhamos, sem perda de generalidade, que $m \geq n$. Se $m = n$, nada há a fazer. Suponhamos, pois, $m > n$ e consideremos o algoritmo de Euclides para m e n:

$$\begin{array}{lcll} m &=& nq_1 + r_1 & 0 < r_1 < n; \\ n &=& r_1q_2 + r_2 & 0 < r_2 < r_1; \\ r_1 &=& r_2q_3 + r_3 & 0 < r_3 < r_2; \\ & & \cdots & \cdots \\ r_{j-2} &=& r_{j-1}q_j + r_j & 0 < r_j < r_{j-1}; \\ r_{j-1} &=& r_jq_{j+1} + 0. & \end{array}$$

Nossa discussão anterior garante que

$$\text{mdc}\,(m,n) = \text{mdc}\,(n, r_1) = \text{mdc}\,(r_1, r_2) = \cdots = \text{mdc}\,(r_{j-1}, r_j) = r_j.$$

Portanto, aplicando a discussão acima sucessivas vezes, concluímos que

$$\begin{aligned} \text{mdc}\,(a^m - 1, a^n - 1) &= \text{mdc}\,(a^n - 1, a^{r_1} - 1) \\ &= \text{mdc}\,(a^{r_1} - 1, a^{r_2} - 1) \\ &\cdots \\ &= \text{mdc}\,(a^{r_{j-1}} - 1, a^{r_j} - 1) \\ &= a^{r_j} - 1 = a^{\text{mdc}\,(m,n) - 1}. \end{aligned}$$

■

Finalizamos esta seção estudando o *mínimo múltiplo comum* de um conjunto finito de inteiros não nulos. Dados inteiros não nulos $a_1, a_2, \ldots, a_n$, o inteiro positivo $|a_1 a_2 \ldots a_n|$ é um múltiplo comum de $a_1, a_2, \ldots, a_n$. Existe, portanto, um menor inteiro positivo que é múltiplo comum de $a_1, a_2, \ldots, a_n$, o que dá sentido à definição a seguir.

Definição 1.29. Dados inteiros não nulos $a_1, a_2, \ldots, a_n$, o **mínimo múltiplo comum** de $a_1, a_2, \ldots, a_n$, denotado $\text{mmc}\,(a_1, a_2, \ldots, a_n)$, é o menor dentre todos os múltiplos positivos comuns de $a_1, a_2, \ldots, a_n$.

Os resultados a seguir estabelecem as propriedades básicas do mmc.

Proposição 1.30. Sejam $a_1, a_2, \ldots, a_n \in \mathbb{Z}^*$ e $m = \text{mmc}\,(a_1, a_2, \ldots, a_n)$. Para todo inteiro M, temos que M é um múltiplo comum de $a_1, a_2, \ldots, a_n$ se, e só se, $m \mid M$.

Prova. Seja M um múltiplo comum de $a_1, a_2, \ldots, a_n$, e escreva $M = mq + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < m$. Como $a_1 \mid m$ e $a_1 \mid M$, segue da proposição 1.5 que $a_1 \mid (M - mq)$, i.e., $a_1 \mid r$; analogamente, $a_2, \ldots, a_n \mid r$, i.e., $0 \leq r < m$ é um múltiplo comum de $a_1, a_2, \ldots, a_n$. Mas, como m é o menor múltiplo comum positivo de $a_1, a_2, \ldots, a_n$, a única possibilidade é termos $r = 0$, de maneira que $m \mid M$. ■

Lema 1.31. Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos. Se $k \in \mathbb{N}$, então $\text{mmc}\,(ka_1, ka_2, \ldots, ka_n) = k\,\text{mmc}\,(a_1, a_2, \ldots, a_n)$.

Prova. Sejam $M = \text{mmc}\,(ka_1, ka_2, \ldots, ka_n)$ e $m = \text{mmc}\,(a_1, a_2, \ldots, a_n)$. Então km é múltiplo de $ka_1, ka_2, \ldots, ka_n$, de modo que $km \geq M$. Por outro lado, como M é um múltiplo comum de $ka_1, ka_2, \ldots, ka_n$, segue que M/k é um múltiplo comum de $a_1, a_2, \ldots, a_n$ e, daí, $M/k \geq m$ ou, ainda, $M \geq km$. Logo, $M = km$. ■

A proposição a seguir relaciona o mdc e o mmc de dois inteiros não nulos.

Proposição 1.32. Se a e b são inteiros não nulos, então

$$\text{mmc}\,(a, b) \cdot \text{mdc}\,(a, b) = |ab|.$$

Prova. Mostremos primeiro que $\text{mdc}\,(a, b) = 1 \Rightarrow \text{mmc}\,(a, b) = |ab|$. Seja m um múltiplo positivo comum de a e b. Como $\text{mdc}\,(a, b) = 1$, o item (e) da proposição 1.21 garante que $ab \mid m$. Portanto, $m \geq |ab|$, de forma que $|ab|$ é o menor múltiplo positivo comum de a e b, ou seja, $|ab| = \text{mmc}\,(a, b)$.

Para o caso geral, note primeiro que $\text{mmc}\,(a, -b) = \text{mmc}\,(a, b)$; como já temos $\text{mdc}\,(a, -b) = \text{mdc}\,(a, b)$, podemos supor, sem perda de generalidade, que $a, b > 0$. Sejam $d = \text{mdc}\,(a, b)$ e u, v inteiros primos entre si e tais que $a = du$, $b = dv$. Queremos mostrar que $\text{mmc}\,(du, dv)d = d^2uv$ ou, ainda, (e pelo lema anterior) que $\text{mmc}\,(u, v) = uv$. Mas isso é exatamente o conteúdo da primeira parte acima. ■

Exemplo 1.33 (Japão)**.** Encontre todos os pares (a, b) de inteiros positivos tais que $a \geq b$ e

$$\text{mmc}\,(a, b) + \text{mdc}\,(a, b) + a + b = ab.$$

Solução. Sejam $d = \text{mdc}\,(a, b)$ e $u, v \in \mathbb{N}$ tais que $a = du$, $b = dv$. Então $u \geq v$ e

$$d \cdot \text{mmc}\,(a, b) = \text{mdc}\,(a, b) \cdot \text{mmc}\,(a, b) = ab = d^2uv,$$

de maneira que $\text{mmc}\,(a, b) = duv$. Substituindo as expressões acima na equação original, concluímos que a mesma equivale a

$$u(v + 1) + (v + 1) = duv, \tag{1.6}$$

de maneira que $u \mid (v+1)$. Assim, $u \leq v+1$ e, daí, $u = v$ ou $u = v+1$. Se $u = v$, segue de $\text{mdc}\,(u, v) = 1$ que $u = v = 1$, de sorte que $d = 4$

e $a = b = 4$. Se $u = v + 1$, segue de (1.6) que

$$\begin{aligned} d &= \frac{u(v+1)+(v+1)}{uv} = \frac{(v+1)^2+(v+1)}{(v+1)v} \\ &= \frac{v^2+3v+2}{v^2+v} = 1 + \frac{2}{v}, \end{aligned}$$

o que implica $v = 1$ ou $v = 2$. Examinando cada caso separadamente, chegamos às demais soluções: $a = 6$, $b = 3$ ou $a = 6$, $b = 4$. ■

Problemas – Seção 1.2

1. (IMO.) Para $n \in \mathbb{N}$, prove que $\operatorname{mdc}(21n+4, 14n+3) = 1$.

2. (OIM.) Sejam m e n inteiros positivos. Se $2^m + 1 = n^2$, prove que $m = n = 3$.

3. Considere duas progressões aritméticas infinitas e não constantes, cujos termos são inteiros positivos. Prove que existem infinitos naturais que são termos de ambas as sequências se, e só se, o mdc de suas razões dividir a diferença entre seus termos iniciais.

4. * Dados $a, m, n \in \mathbb{N}$, com $m \neq n$, prove que $\operatorname{mdc}(a^{2^n}+1, a^{2^m}+1) = 1$ ou 2.

5. (Japão.) Prove que $\operatorname{mdc}(n!+1, (n+1)!+1) = 1$, para todo $n \in \mathbb{N}$.

6. (Torneio das Cidades.) Se a e b são números naturais tais que $ab \mid (a^2+b^2)$, mostre que $a = b$.

7. (OBM.) Dados $a, b \in \mathbb{N}$, particione um retângulo $a \times b$ em ab quadradinhos 1×1. Prove que cada diagonal do retângulo passa pelo interior de exatamente $a+b-\operatorname{mdc}(a,b)$ quadradinhos 1×1.

8. Sejam n e k inteiros positivos, com $n \geq k$. Prove que o mdc dos números
$$\binom{n}{k}, \binom{n+1}{k}, \ldots, \binom{n+k}{k}$$
é igual a 1.

9. Seja $n > 1$ um inteiro tal que 2^k é a maior potência de 2 que divide n. Prove que o máximo divisor comum dos números binomiais
$$\binom{2n}{1}, \binom{2n}{3}, \binom{2n}{5}, \ldots, \binom{2n}{2n-1}$$

é igual a 2^{k+1}.

10. (Estados Unidos - adaptado.) Fixado $k \in \mathbb{N}$, mostre que

$$\max\{\operatorname{mdc}(n^2+k,(n+1)^2+k);\, n \in \mathbb{N}\} = 4k+1.$$

11. Se a, b e c são inteiros positivos tais que $\frac{1}{a}+\frac{1}{b}=\frac{1}{c}$, prove que existem inteiros positivos q, u e v tais que $\operatorname{mdc}(u,v)=1$ e $a=qu(u+v)$, $b=qv(u+v)$ e $c=quv$.

12. (Inglaterra.) Sejam x,y naturais tais que $2xy$ divide x^2+y^2-x. Prove que x é um quadrado perfeito.

13. (Estados Unidos.) De qualquer conjunto de 10 naturais consecutivos, prove que é sempre possível escolher ao menos um que seja relativamente primo com os nove restantes.

$mdc(y,z)=1$.

14. Sejam a, b e m naturais dados, com $\operatorname{mdc}(a,m)=1$. Mostre que

$$\sum_{j=0}^{m-1}\left\lfloor \frac{aj+b}{m}\right\rfloor = \frac{1}{2}(a-1)(m-1)+b.$$

Para o problema a seguir, recorde (cf. problema 1.1.7 do volume 3) que, dado $x \in \mathbb{R}$, sua *parte fracionária* é o real $\{x\}$, tal que $\{x\}=x-\lfloor x\rfloor$. Assim, $\{x\}\in[0,1)$ e $\{x\}=0 \Leftrightarrow x\in\mathbb{Z}$.

15. (Japão.) Sejam $n,r \in \mathbb{N}$ tais que $n>1$ e $n \nmid r$. Se $g=\operatorname{mdc}(n,r)$, prove que

$$\sum_{i=1}^{n-1}\left\{\frac{ri}{n}\right\} = \frac{1}{2}(n-g).$$

16. (Putnam.) Dados $m,n \in \mathbb{N}$, com $m \geq n$, prove que o número $\frac{\operatorname{mdc}(m,n)}{m}\binom{m}{n}$ é um natural.

17. (Bulgária.) Seja $(a_n)_{n\geq 1}$ a sequência de inteiros positivos definida por $a_1=2$ e, para todo $n\in\mathbb{N}$, $a_{n+1}=a_n^2-a_n+1$. Mostre que dois termos quaisquer dessa sequência são primos entre si.

18. * Seja $(F_n)_{n\geq 1}$ a sequência de Fibonacci, i.e., a sequência tal que $F_1=F_2=1$ e $F_{k+2}=F_{k+1}+F_k$, para todo $k\in\mathbb{N}$. Nosso objetivo neste problema é provar que $\operatorname{mdc}(F_m,F_n)=F_{\operatorname{mdc}(m,n)}$. Para tanto, faça os seguintes itens:

    (a) Prove que, para todo $n\in\mathbb{N}$, tem-se $\operatorname{mdc}(F_n,F_{n+1})=1$.

    (b) Prove que, para todos $n,k\in\mathbb{N}$, com $n>1$, tem-se $F_{n+k}=F_{n-1}F_k+F_nF_{k+1}$.

    (c) Use o item (b) para concluir que, para todos $n,q,r\in\mathbb{N}$,

    (i) $\operatorname{mdc}(F_{nq},F_n)=F_n$.

    (ii) $\operatorname{mdc}(F_{nq-1},F_n)=1$.

    (iii) $\operatorname{mdc}(F_{nq+r},F_n)=\operatorname{mdc}(F_r,F_n)$.

    (d) Conclua que $\operatorname{mdc}(F_n,F_m)=F_{\operatorname{mdc}(m,n)}$ para todos m e n naturais.

19. (Croácia.) Seja $(a_n)_{n\geq 1}$ uma sequência de números inteiros tal que $a_1=1$ e $a_{n+2}=a_2a_{n+1}+a_n$, para todo $n\in\mathbb{N}$. Prove que $\operatorname{mdc}(a_m,a_n)=a_{\operatorname{mdc}(m,n)}$.

20. Dados $a,b\in\mathbb{N}$ primos entre si, prove os seguintes itens:

    (a) Todo natural $n>ab$ pode ser escrito da forma $n=ax+by$, com x,y naturais.

    (b) O inteiro ab não pode ser escrito como em (a).

    (c) Todo inteiro $n>ab-a-b$ pode ser escrito da forma $n=ax+by$, com x,y inteiros não negativos.

    (d) O inteiro $ab-a-b$ não pode ser escrito como em (c).

(e) Há exatamente $\frac{1}{2}(a-1)(b-1)$ inteiros não negativos que não podem ser escritos da forma $ax+by$, com x e y também inteiros não negativos.

21. (IMO - adaptado.) Sejam a, b, c naturais dois a dois primos entre si.

(a) Mostre que não existem $x, y, z \in \mathbb{Z}_+$ tais que $2abc - ab - bc - ca = xbc + yac + zab$.

(b) Se $n \in \mathbb{N}$ é tal que $n > abc - a - bc$, use o resultado do problema anterior para concluir pela existência de $x, t \in \mathbb{Z}_+$ tais que $n = xbc + ta$, com $0 \leq x \leq a - 1$.

(c) Mostre que o inteiro t do item (b) é maior que $bc-b-c$, e use novamente o resultado do problema anterior para concluir pela existência de $y, z \in \mathbb{Z}_+$ tais que $t = bz + cy$.

(d) Se $n \in \mathbb{N}$ é tal que $n > 2abc - ab - bc - ca$, use os itens (b) e (c) para mostrar que existem $x, y, z \in \mathbb{Z}_+$ tais que $n = xbc + yac + zab$.

22. Generalize o resultado do problema anterior do seguinte modo: se $a_1, a_2, \ldots, a_n$ são naturais dois a dois primos entre si e

$$A = \left\{ \sum_{j=1}^{n} x_j a_1 \cdots \widehat{a}_j \cdots a_n \,|\, x_1, \ldots, x_n \in \mathbb{Z}_+ \right\}$$

($\widehat{a}_j$ indica que a_j não está presente no produto $x_j a_1 \cdots \widehat{a}_j \cdots a_n$), então o maior natural que não pertence a A é o número

$$\left(n - 1 - \sum_{i=1}^{n} \frac{1}{a_i} \right) \prod_{i=1}^{n} a_i.$$

23. É interessante nos perguntarmos sobre a eficiência do algoritmo de Euclides para o cálculo do mdc de dois inteiros não nulos.

Informações sobre essa questão nos são dadas por um teorema devido ao matemático francês Gabriel Lamé, e o objetivo deste problema é prová-lo. Para tanto, faça os seguintes itens:

(a) Se F_k é o $k-$ésimo número de Fibonacci e $n \in \mathbb{N}$, prove que $F_{n+5} > 10F_n$ e deduza, a partir daí, que $F_{5n+2} > 10^n$, de modo que F_{5n+2} tem pelo menos $n+1$ algarismos em sua representação decimal.

(b) Se n passos forem usados no algoritmo de Euclides para calcular $\text{mdc}\,(a, b)$, com $a > b > 0$ e usando b como o primeiro divisor, prove que $b \geq F_{n-1}$.

(c) Prove o **teorema de Lamé**: o número de divisões necessárias, no algoritmo de Euclides, para calcularmos o mdc de dois inteiros positivos é, no máximo, cinco vezes o número de algarismos da representação decimal do menor dos dois números.

24. (OBM.) Seja $n > 1$ inteiro. Prove que o número

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

nunca é inteiro.

1.3 Números primos

Um inteiro $p > 1$ é **primo** se seus únicos divisores positivos forem 1 e p. Um inteiro $a > 1$ que não é primo é dito **composto**. Provaremos logo mais (cf. teorema 1.37) que o conjunto dos números primos é infinito; por ora, para comodidade do leitor, listamos abaixo os números primos menores que 50, cujas primalidades podem ser verificadas sem dificuldade:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

Nosso objetivo nesta seção é estudar os números primos e sua relação com os números compostos. Começamos com o seguinte resultado auxiliar, conhecido como o **lema de Euclides**.

Lema 1.34 (Euclides). Todo inteiro $n > 1$ pode ser expresso como o produto de um número finito de primos, não necessariamente distintos[2].

Prova. Façamos a prova por indução sobre n. Se $n = 2$, nada há a fazer (uma vez que 2 é primo). Suponha, agora, que todo inteiro n tal que $2 \leq n < m$ pode ser escrito como o produto de um número finito de primos; provemos que este é também o caso para m: se m for primo, nada há a fazer. Senão, existem inteiros a e b tais que $m = ab$, com $1 < a, b < m$. Pela hipótese de indução, a e b podem ser escritos como produtos de números finitos de primos, digamos $a = p_1 \ldots p_k$, $b = q_1 \cdots q_l$, com $k, l \geq 1$ e $p_1, \ldots, p_k$, $q_1, \ldots, q_l$ primos. Logo, $m = ab = p_1 \ldots p_k q_1 \cdots q_l$, também o produto de um número finito de primos. ■

Como corolário do lema acima, temos o seguinte critério de pesquisa de divisores primos de um número composto, devido ao matemático grego Eratóstenes de Cirene (cf. figura 1.2).

Corolário 1.35 (Eratóstenes). Se um inteiro $n > 1$ for composto, então n possui um divisor primo p, tal que $p \leq \sqrt{n}$.

Prova. Seja $n = ab$, com $1 < a \leq b$. Sendo p um divisor primo de a, segue que $p \mid n$ e

$$p^2 \leq a^2 \leq ab = n,$$

de modo que $p \leq \sqrt{n}$. ■

Exemplo 1.36. Use o corolário acima para provar que 641 é primo.

[2]Conforme estabelecido na definição 4.21 do volume 1, identificamos o produto $\prod_{i=1}^{1} a_i$ com a_1.

Prova. Inicialmente, note que $25 < \sqrt{641} < 26$. Portanto, se 641 for composto, segue do corolário acima que 641 deve possuir um divisor primo $p \leq 25$, de modo que

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23\}.$$

No entanto, é imediato verificar que, dentre as divisões de 641 pelos primos acima, nenhuma é exata. Logo, 641 é primo. ■

A utilização do corolário 1.35 para decidir se um certo natural é primo (como no exemplo acima) é conhecida como o **crivo de Eratóstenes**. De maneira geral, basta dividir o natural em questão por todos os primos menores ou iguais que sua raiz quadrada por falta; de acordo com o corolário, se nenhuma dessas divisões for exata, o número será primo. Mais que interesse prático, contudo, a maior utilidade do crivo de Eratóstenes é teórica, uma vez que, para aplicá-lo para decidir se 999997 é primo, por exemplo, teríamos de dividi-lo por todos os primos menores ou iguais a $\sqrt{999997} \cong 1000$, o que não é razoável[3].

De volta ao lema 1.34, reunindo primos iguais concluímos que é possível escrever todo inteiro $n > 1$ na forma $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, onde $p_1, \ldots, p_k$ são primos dois a dois distintos e $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Veremos no teorema 1.42 que, a menos de uma reordenação de fatores, essa maneira de escrever n é única. Antes, contudo, provemos que o conjunto dos números primos é infinito, resultado este também devido a Euclides.

Teorema 1.37 (Euclides). O conjunto dos números primos é infinito.

[3]Com um pouco mais de trabalho, é possível mostrar que o crivo de Eratóstenes é um algoritmo que, genericamente, não termina em *tempo polinomial.* De outra forma, isto significa que a quantidade de operações que necessitamos executar para encontrar o n−ésimo primo com o auxílio do crivo de Eratóstenes cresce exponencialmente com n, de forma que mesmo com o auxílio de um computador esse não é um bom *algoritmo de primalidade.*

Figura 1.2: Eratóstenes de Cirene, matemático grego do século II a.C. Além de seu algoritmo de primalidade, outro trabalho notável de Eratóstenes foi conseguir medir indiretamente o diâmetro da Terra, com precisão impressionante para a época.

Prova. Por indução sobre n, provemos que, se $\mathbb{N}$ contiver n primos distintos, então $\mathbb{N}$ conterá $n+1$ primos distintos. Suponha que $p_1, \ldots, p_n$ são primos distintos, e seja

$$m = p_1 \ldots p_n + 1.$$

Pelo lema 1.34, existe um primo p tal que $p \mid m$. Se $p = p_i$ para algum $1 \leq i \leq n$, então $p \mid p_1 \ldots p_n$ e segue da proposição 1.5 que p divide a diferença $m - p_1 \ldots p_n$, i.e., $p \mid 1$, o que é um absurdo. Logo, p é um primo diferente de todos os p_i's, de maneira que temos pelo menos $n+1$ primos distintos em $\mathbb{N}$. ■

Observação 1.38. Em que pese o resultado acima, há lacunas arbitrariamente grandes na sequência dos primos. De fato, dado $k \geq 3$ inteiro, para que os inteiros positivos e consecutivos $a+2, a+3, \ldots, a+k$ sejam todos compostos basta que a seja um múltiplo comum dos números $2, 3, \ldots, k$.

Teremos mais a dizer sobre a distribuição dos números primos ao longo dos naturais no capítulo 4.

A utilização de pequenas variações do argumento usado na prova do teorema de Euclides nos permite mostrar que várias PA's contêm uma infinitude de números primos. Vejamos um exemplo nesse sentido[4].

Exemplo 1.39. Prove que há infinitos primos da forma $4k - 1$.

Prova. Suponha que só houvesse uma quantidade finita de primos da forma $4k - 1$, digamos $p_1 = 3, p_2 = 7, p_3 = 11, \ldots, p_t$, e considere o número

$$m = 4p_1p_2 \ldots p_t - 1.$$

Claramente, $m > 1$ e, sendo $m' = p_1p_2 \ldots p_t$, temos $m = 4m' - 1$. Por outro lado, o lema 1.34 garante a existência de primos ímpares $q_1, \ldots, q_l$ tais que $m = q_1 \ldots q_l$. Observe, agora, que todo primo ímpar é da forma $4q' - 1$ ou $4q' + 1$, para algum $q' \in \mathbb{Z}$. Se fosse $q_i = 4q_i' + 1$ para $1 \leq i \leq t$, teríamos

$$m = (4q_1' + 1) \ldots (4q_l' + 1) = 4q + 1,$$

para algum $q \in \mathbb{N}$, contradizendo o fato de ser $m = 4m' - 1$. Portanto, existe $1 \leq i \leq l$ tal que $q_i = 4q_i' - 1$. Finalmente, como $p_1, p_2, \ldots, p_t$ são todos os primos dessa forma, deveríamos ter $q_i = p_j$ para algum $1 \leq j \leq t$. Mas, como $q_i \mid m$, seguiria então que p_j seria um divisor do número $m = 4p_1p_2 \ldots p_t - 1$, o que é uma contradição. ■

Para a prova do teorema 1.42, precisamos do lema a seguir, o qual apresenta interesse próprio.

[4]É possível provar um resultado muito mais geral, devido ao matemático alemão do século XIX Gustav Lejeune Dirichlet, o qual afirma que toda PA infinita e não constante de números naturais contém infinitos números primos, contanto que seu primeiro termo e sua razão sejam primos entre si. Veremos um caso particular relevante desse teorema na seção 8.2 do volume 6.

Lema 1.40. Se $a_1, \ldots, a_n \in \mathbb{N}$ e p é um primo tal que $p \mid a_1 a_2 \ldots a_n$, então existe $1 \leq i \leq n$ tal que $p \mid a_i$. Em particular, se $a_1, \ldots, a_n$ forem todos primos, então existe $1 \leq i \leq n$ tal que $p = a_i$.

Prova. Façamos a prova no caso $n = 2$, sendo o caso geral totalmente análogo. Suponha que $p \mid (ab)$ mas $p \nmid a$, e seja $d = \text{mdc}\,(a, p)$. Como $d \mid p$, temos $d = 1$ ou $d = p$; mas $p \nmid a$ e $d \mid a$ garantem que $d \neq p$, i.e., $d = 1$. Assim, como $p \mid (ab)$ e $\text{mdc}\,(a, p) = 1$, segue do item (a) da proposição 1.21 que $p \mid b$. O resto é imediato a partir da definição de número primo. ∎

Exemplo 1.41. Se p é um primo ímpar, então p divide cada um dos números

$$\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}.$$

Prova. Seja $1 \leq k \leq p - 1$. Uma vez que o número

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{(k+1)\ldots(p-1)p}{(p-k)!}$$

é um inteiro, temos que $(p-k)!$ divide $(k+1)\ldots(p-1)p$. Agora, como p é primo e $p \nmid 1, 2, \ldots, p-k$, o lema anterior garante que $p \nmid (p-k)!$, de sorte que $\text{mdc}\,(p, (p-k)!) = 1$. Portanto, pelo item (a) da proposição 1.21 concluímos que $(p-k)!$ divide $(k+1)\ldots(p-1)$ e, daí,

$$\binom{p}{k} = \underbrace{\frac{(k+1)\ldots(p-1)}{(p-k)!}}_{\in \mathbb{N}} \cdot p,$$

um múltiplo de p. ∎

O teorema a seguir é a pedra fundamental da teoria elementar dos números, sendo conhecido como o **teorema fundamental da aritmética**.

Teorema 1.42. Todo inteiro $n > 1$ pode ser escrito como o produto de potências de primos distintos. Ademais, tal decomposição de n é única no seguinte sentido: se $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k} = q_1^{\beta_1} \ldots q_l^{\beta_l}$, onde $p_1 < \cdots < p_k$ e $q_1 < \cdots < q_l$ são números primos e $\alpha_i, \beta_j \geq 1$ são inteiros, então $k = l$ e, para $1 \leq i \leq k$, $p_i = q_i$ e $\alpha_i = \beta_i$.

Prova. A parte de existência foi estabelecida no parágrafo anterior ao teorema 1.37. Para a unicidade, suponha que o inteiro $n > 1$ admite duas decomposições como no enunciado. Como $p_1 \mid n$, temos que $p_1 \mid q_1^{\beta_1} \ldots q_l^{\beta_l}$, e o lema anterior garante a existência de $1 \leq j \leq l$ tal que $p_1 = q_j$. Por outro lado, como $q_1 \mid n$, temos que $q_1 \mid p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ e, novamente pelo lema anterior, existe $1 \leq i \leq k$ tal que $q_1 = p_i$. Assim, $p_1 = q_j \geq q_1 = p_i \geq p_1$, de onde segue que $p_1 = q_1$ e, daí,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = p_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}.$$

Provemos agora que $\alpha_1 = \beta_1$. Se $\alpha_1 < \beta_1$, então $p_2^{\alpha_2} \ldots p_k^{\alpha_k} = p_1^{\beta_1 - \alpha_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$, de maneira que $p_1 \mid p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Mas aí, argumentando como acima, existiria $2 \leq i \leq k$ tal que $p_1 = p_i$, o que é um absurdo. Analogamente, não pode ser $\alpha_1 > \beta_1$. Logo, $\alpha_1 = \beta_1$ e segue que

$$p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_2^{\beta_2} \ldots q_l^{\beta_l}.$$

Repetindo o argumento acima várias vezes (há uma indução embutida aqui, a qual não formalizaremos a bem da clareza do argumento), concluímos sucessivamente que $p_2 = q_2$ e $\alpha_2 = \beta_2$, $p_3 = q_3$ e $\alpha_3 = \beta_3$, etc. Ao final, se $k < l$, obteremos $1 = q_{k+1}^{\beta_{k+1}} \ldots q_l^{\beta_l}$, o que é claramente um absurdo; se $k > l$, obtemos um absurdo análogo. Logo, $k = l$ e nada mais há a fazer. ∎

Exemplo 1.43. Os naturais x e y são tais que $3x^2 + x = 4y^2 + y$. Prove que $x - y$ é um quadrado perfeito.

Prova. Sejam p um primo e p^a, p^b e p^c as maiores potências de p que dividem x, y e $x - y$, respectivamente. Suponha, por um momento,

que $a \leq b$. Então $p^{2a} \mid x^2, y^2$, e segue do item (c) da proposição 1.5 que $p^{2a} \mid (4y^2 - 3x^2)$. Mas, como $x - y = 4y^2 - 3x^2$, temos então que $p^{2a} \mid (x - y)$ e, daí, $c \geq 2a$. Por outro lado, escrevendo

$$x^2 = (x - y) - 4(y^2 - x^2) = (x - y)[1 + 4(y + x)],$$

concluímos que $p^c \mid x^2$, de modo que (argumentando como acima) $c \leq 2a$. Portanto, $c = 2a$, um número par. Se $a \geq b$, concluímos, de modo análogo, que $c = 2b$.

Por fim, como o primo p foi escolhido arbitrariamente, segue do teorema fundamental da aritmética que $x - y$ é um produto de potências de primos com expoentes pares, logo um quadrado perfeito. ■

A representação de um inteiro $n > 1$ como um produto de potências de primos distintos é sua **fatoração** ou **decomposição canônica** em fatores primos. Os corolários a seguir colecionam algumas consequências úteis da existência de uma tal fatoração.

Corolário 1.44. Sejam a, b, m e n naturais tais que $a^m = b^n$. Se $\text{mdc}\,(m, n) = 1$, então existe $c \in \mathbb{N}$ tal que $a = c^n$ e $b = c^m$.

Prova. É claro que a e b são divisíveis exatamente pelos mesmos primos, $p_1, \ldots, p_k$ digamos. Sejam $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} \ldots p_k^{\beta_k}$, com $\alpha_i, \beta_i \geq 1$, as decomposições canônicas de a e b. Então,

$$p_1^{m\alpha_1} \ldots p_k^{m\alpha_k} = a^m = b^n = p_1^{n\beta_1} \ldots p_k^{n\beta_k}$$

e a parte de unicidade do teorema fundamental da aritmética garante que

$$m\alpha_i = n\beta_i, \quad \forall \; 1 \leq i \leq k. \tag{1.7}$$

Assim, $m \mid n\beta_i$ e, como m e n são primos entre si, o item (a) da proposição 1.21 permite concluir que $m \mid \beta_i$. Se $u_i \in \mathbb{N}$ é tal que $\beta_i = mu_i$, segue de (1.7) que $\alpha_i = nu_i$; portanto, sendo $c = p_1^{u_1} \ldots p_k^{u_k}$, temos

$$a = p_1^{nu_1} \ldots p_k^{nu_k} = c^n \quad \text{e} \quad b = p_1^{mu_1} \ldots p_k^{mu_k} = c^m.$$

■

Vejamos, agora, como obter as decomposições canônicas dos divisores de um inteiro maior que 1 e do mdc e mmc de dois inteiros não nulos.

Corolário 1.45. Se $n = p_1^{\beta_1} \ldots p_k^{\beta_k}$ é a decomposição canônica do inteiro $n > 1$, então os divisores positivos de n são os números da forma $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, com $0 \leq \alpha_i \leq \beta_i$, para $1 \leq i \leq k$. Em particular, denotando por $d(n)$ o número de divisores positivos de n, temos

$$d(n) = \prod_{i=1}^{k} (\beta_i + 1). \tag{1.8}$$

Prova. Se $d > 1$ é divisor de n e p é um primo que divide d, então p também divide n, de forma que p é igual a um dos primos $p_1, \ldots, p_k$. Mas, como isso é válido para todo divisor primo de d, segue que $d = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, com $\alpha_i \geq 0$ para todo i (não escrevemos $\alpha_i \geq 1$ pois pode ocorrer que $p_i \nmid d$ para um ou mais valores de i). Agora, se $q \in \mathbb{N}$ é tal que $n = dq$, então

$$p_1^{\alpha_1} \ldots p_k^{\alpha_k} q = p_1^{\beta_1} \ldots p_k^{\beta_k},$$

e a parte de unicidade do teorema fundamental da aritmética permite concluir facilmente que $\alpha_i \leq \beta_i$ para todo i. Reciprocamente, é imediato que todo natural d da forma $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, com $0 \leq \alpha_i \leq \beta_i$ para $1 \leq i \leq k$, é um divisor positivo de n.

Para o que falta, o que fizemos acima, novamente em conjunção com a parte de unicidade do teorema fundamental da aritmética, garante que o número de divisores positivos de n coincide com o número de sequências $(\alpha_1, \ldots, \alpha_k)$ de inteiros tais que $0 \leq \alpha_i \leq \beta_i$ para $1 \leq i \leq k$. Como há $\beta_i + 1$ possibilidades para α_i, a fórmula (1.8) segue do princípio fundamental da contagem (cf. corolário 1.9 do volume 4). ■

Vejamos um exemplo de aplicação do resultado acima.

Exemplo 1.46. Prove que um natural n é quadrado perfeito se, e só se, $d(n)$ for ímpar.

Prova. Primeiramente, como $1 = 1^2$ e $d(1) = 1$ é ímpar, podemos supor que $n > 1$. Seja, então, $n > 1$ um inteiro e $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ sua decomposição canônica em fatores primos. Se n for quadrado perfeito, então, para $1 \leq i \leq k$, existe $\beta_i \in \mathbb{N}$ tal que $\alpha_i = 2\beta_i$. Portanto, o corolário anterior fornece

$$\begin{aligned} d(n) &= (\alpha_1 + 1) \ldots (\alpha_k + 1) \\ &= (2\beta_1 + 1) \ldots (2\beta_k + 1), \end{aligned}$$

um número ímpar. A recíproca é análoga. ■

Para o próximo corolário, é útil estendermos a decomposição canônica de um inteiro maior que 1 em primos permitindo expoentes iguais a 0. Por exemplo, podemos escrever $48 = 2^4 \cdot 3$ e $270 = 2 \cdot 3^3 \cdot 5$ utilizando os primos 2, 3 e 5 em ambos os casos, i.e., escrevendo

$$48 = 2^4 \cdot 3 \cdot 5^0 \text{ e } 270 = 2 \cdot 3^3 \cdot 5.$$

Corolário 1.47. Sejam $a, b > 1$ naturais dados, com $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ e $b = p_1^{\beta_1} \ldots p_k^{\beta_k}$, onde $p_1 < \cdots < p_k$ são números primos e $\alpha_i, \beta_i \geq 0$ para $1 \leq i \leq k$. Então

$$\text{mdc}\,(a, b) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i\}} \quad \text{e} \quad \text{mmc}\,(a, b) = \prod_{i=1}^{k} p_i^{\max\{\alpha_i, \beta_i\}}.$$

Prova. Façamos a prova para o mcd (a prova para o mmc é análoga). Como $\min\{\alpha_i, \beta_i\} \leq \alpha_i, \beta_i$ para todo i, temos que o número $d = \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i\}}$ divide ambos a e b. Seja, agora, d' um divisor positivo qualquer de a e b. Pelo corolário 1.45, a decomposição em primos de d' é da forma $d' = p_1^{\gamma_1} \ldots p_k^{\gamma_k}$, com $\gamma_i \geq 0$ para todo i. Mas, $d' \mid a$ implica $\gamma_i \leq \alpha_i$ e $d' \mid b$ implica $\gamma_i \leq \beta_i$. Assim, para todo i, temos $\gamma_i \leq \min\{\alpha_i, \beta_i\}$, de modo que $d' \mid d$. Logo, $d = \text{mdc}\,(a, b)$. ■

De volta ao parágrafo anterior ao corolário, agora podemos calcular imediatamente

$$\text{mdc}\,(48, 270) = 2 \cdot 3 = 6 \quad \text{e} \quad \text{mmc}\,(48, 270) = 2^4 \cdot 3^3 \cdot 5 = 2160.$$

Suponha que saibamos que um certo natural n admite um divisor primo p. A proposição a seguir, devido ao matemático francês Adrien-Marie Legendre[5], ensina como calcular o expoente de p na decomposição canônica de n em fatores primos, mesmo que não conheçamos tal decomposição explicitamente. A fórmula (1.9) é conhecida como a **fórmula de Legendre**.

Proposição 1.48. Sejam $n > 1$ natural e p primo. Se $e_p(n)$ denota o expoente de p na decomposição canônica de $n!$, então

$$e_p(n) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor. \tag{1.9}$$

Prova. Note, inicialmente, que a soma acima é sempre finita, uma vez que, para $p^k > n$, temos $\lfloor \frac{n}{p^k} \rfloor = 0$. Seja $k \in \mathbb{N}$ qualquer e $p^k, 2p^k, \ldots, mp^k$ os múltiplos de p^k menores ou iguais a n. Então $mp^k \leq n < (m+1)p^k$ ou, equivalentemente, $m \leq \frac{n}{p^k} < m + 1$. Portanto, m é o maior inteiro menor ou igual a $\frac{n}{p^k}$, quer dizer, $m = \lfloor \frac{n}{p^k} \rfloor$. Assim, para cada $k \geq 1$ há exatamente

$$\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$$

naturais menores ou iguais a n e que são múltiplos de p^k mas não de p^{k+1}. Mas, como cada um de tais números contribui com exatamente k fatores p para $e_p(n)$, segue que

$$e_p(n) = \sum_{k \geq 1} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

■

[5] Matemático francês dos séculos XVIII e XIX.

Os dois exemplos a seguir trazem aplicações interessantes da fórmula de Legendre.

Exemplo 1.49 (União Soviética). Ache o número de zeros consecutivos no final do número 1000!.

Prova. Escrevendo $1000! = 2^{e_2(1000)} \cdot 5^{e_5(1000)} m$, com $m \in \mathbb{N}$, vemos que basta calcular o menor dos números $e_2(1000)$ e $e_5(1000)$ a fim de encontrar a maior potência de 10 que divide 1000!. Por outro lado, o menor de tais números é claramente $e_5(1000)$, o qual pode ser calculado por intermédio da fórmula de Legendre, levando em conta que $5^5 > 1000$:

$$e_5(1000) = \sum_{j=1}^{4} \left\lfloor \frac{1000}{5^j} \right\rfloor = 200 + 40 + 8 + 1 = 249.$$

Logo, 1000! termina em 249 zeros. ■

Exemplo 1.50 (Iugoslávia). Prove que $2^n \nmid n!$, para cada $n \in \mathbb{N}$.

Prova. O resultado é claramente verdadeiro para $n = 1$. Para $n > 1$, o teorema de Legendre garante que a maior potência de 2 que divide $n!$ tem expoente $k = \sum_{j \geq 1} \lfloor \frac{n}{2^j} \rfloor$. Mas, como $\lfloor x \rfloor \leq x$ para todo x e $\lfloor \frac{n}{2^j} \rfloor = 0$ para todo j suficientemente grande, segue que

$$k = \sum_{j \geq 1} \left\lfloor \frac{n}{2^j} \right\rfloor < \sum_{j \geq 1} \frac{n}{2^j} = n,$$

onde utilizamos a fórmula para a soma dos termos de uma série geométrica (cf. proposição 3.21 do volume 3) na última igualdade acima. Logo, $k < n$, de sorte que $2^n \nmid n!$. ■

Problemas – Seção 1.3

1. Sejam p e q primos ímpares consecutivos. Prove que existem inteiros $a, b, c > 1$, não necessariamente distintos, tais que $p+q = abc$.

2. (IMO - adaptado.) Seja $k \in \mathbb{N}$ tal que $p = 3k + 2$ é primo. Se m e n são naturais tais que

$$\frac{m}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{2k} + \frac{1}{2k+1},$$

prove que $p \mid m$.

3. (Hungria.) Dado $p > 2$ primo, ache todos os $x, y \in \mathbb{N}$ tais que $\frac{2}{p} = \frac{1}{x} + \frac{1}{y}$.

4. (IMO.) Ache todos os $n \in \mathbb{N}$ tais que $n(n+1)(n+2)(n+3)$ tenha exatamente três divisores primos distintos.

5. (Rússia.) Seja $(a_n)_{n \geq 1}$ uma sequência de números naturais tais que $\mathrm{mdc}\,(a_i, a_j) = \mathrm{mdc}\,(i, j)$ sempre que $i \neq j$. Prove que $a_n = n$, para todo $n \geq 1$.

6. * Dizemos que um natural n é **livre de quadrados** se $n = 1$ ou $n = p_1 \ldots p_k$, com $p_1 < \cdots < p_k$ primos. Faça os seguintes itens:

   (a) Prove que todo inteiro $n > 1$ pode ser unicamente escrito na forma $n = ab^2$, com a livre de quadrados e b natural.

   (b) Use o item (a) para mostrar que, se existissem exatamente k números primos, então haveria exatamente 2^k inteiros livres de quadrados e que o número de inteiros positivos menores ou iguais a n seria, no máximo, $2^k\sqrt{n}$.

   (c) Use o item (b) para dar outra prova da infinitude dos primos.

7. Mostre que há infinitos primos de cada uma das formas $3k+2$ e $6k+5$.

8. (Iugoslávia.) Para cada $n \in \mathbb{N}$, prove que o número $2^{2^n}-1$ tem ao menos n fatores primos distintos.

9. Se p é um primo ímpar, prove que p divide $\binom{2p}{p}-2$.

10. * Sejam a e n inteiros positivos, com $a>1$. Faça os itens a seguir:

    (a) Se a^n+1 é primo, então n é uma potência de 2 (veremos no problema 6, página 130, que a recíproca não é verdadeira).

    (b) Se $n>1$ e a^n-1 é primo, então n é primo e $a=2$ (a recíproca não é verdadeira, conforme atesta o exemplo $2^{11}-1=23\cdot 89$).

11. (IMO.) Ache todos os $n \in \mathbb{N}$, $n>6$, tais que os naturais menores que n e primos com n formem uma progressão aritmética.

12. (IMO.) Sejam k,m,n naturais tais que $m+k+1$ é um primo maior que $n+1$. Se $c_s=s(s+1)$ para cada $s\in\mathbb{N}$, prove que

$$(c_{m+1}-c_k)(c_{m+2}-c_k)\dots(c_{m+n}-c_k)$$

é divisível por $c_1c_2\cdots c_n$.

13. (Hungria.) Seja n um natural dado. Mostre que há exatamente $d(n^2)$ pares ordenados (u,v) tais que $u,v\in\mathbb{N}$ e $\text{mmc}\,(u,v)=n$.

14. (IMO.) Ache todos os naturais a e b tais que $a^{b^2}=b^a$.

15. (BMO.) Encontre todos os $n\in\mathbb{N}$ tais que $n=d_1^2+d_2^2+d_3^2+d_4^2$, onde $1=d_1<d_2<d_3<d_4$ são os quatro menores divisores positivos de n.

16. (OIM.) Para cada $n\in\mathbb{N}$, sejam $1=d_1<\cdots<d_k=n$ os divisores positivos de n. Encontre todos os n satisfazendo as seguintes condições:

    (a) $k\geq 15$.

    (b) $n=d_{13}+d_{14}+d_{15}$.

    (c) $(d_5+1)^3=d_{15}+1$.

17. (Japão.)[6] Para cada inteiro $n>1$, sejam $I(n)$ a soma dos maiores divisores ímpares dos números $1,2,\dots,n$ e $T(n)=1+2+\cdots+n$. Prove que existem infinitos valores de n para os quais $3I(n)=2T(n)$.

18. (Austrália.) Ache todos os naturais n para os quais $d(n)=\frac{n}{3}$.

19. (IMO.) Sejam m,n inteiros não negativos arbitrários. Prove que o número

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

sempre é um inteiro.

20. Para cada inteiro positivo n, seja $a_n=\binom{2n}{n}$.

    (a) Mostre que o número binomial a_n é sempre par.

    (b) Prove que $4\mid a_n$ se, e só se, n não é potência de 2.

21. (Romênia.) Seja n um natural cuja representação binária tem exatamente k algarismos 1. Prove que 2^{n-k} divide $n!$.

22. Ache todos os naturais a, b e k tais que a e b sejam primos entre si e $(a+kb)(b+ka)$ seja uma potência de um primo.

23. (OBM - adaptado.) Para cada inteiro $n>1$, seja $p(n)$ o maior divisor primo de n. Faça os seguintes itens:

[6] Para a recíproca deste problema, veja o problema 5, página 98.

(a) Se q é um primo ímpar, prove que não podemos ter $p(q^{2^k}) > p(q^{2^k}+1)$ para todo inteiro $k \geq 0$.

(b) Se $p(q^{2^k}) < p(q^{2^k}+1)$ e k é mínimo com tal propriedade, mostre que $p(q^{2^k}-1) < p(q^{2^k})$.

(c) Mostre que existem infinitos naturais n tais que $p(n-1) < p(n) < p(n+1)$.

24. (OBM.) Mostre que existe um conjunto A, formado por inteiros positivos e tendo as seguintes propriedades:

 (a) A tem 1000 elementos.

 (b) A soma de qualquer quantidade de elementos distintos de A (pelo menos um) não é uma potência perfeita de expoente maior que 1.

25. Seja $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ a sequência dos números primos. Para cada $k \in \mathbb{N}$, sejam $x_k = p_1 p_2 \ldots p_k + 1$ e $A = \{x_1, x_2, \ldots\}$. Fixado $m \in \mathbb{N}$, prove que podemos escolher um subconjunto B do conjunto A satisfazendo as seguintes propriedades:

 (a) $|B| = m$.

 (b) Dois elementos quaisquer de B são primos entre si.

 (c) A soma dos elementos de qualquer subconjunto de B com mais de um elemento não é um número primo.

CAPÍTULO 2

Equações Diofantinas

Nosso propósito neste capítulo é estudar algumas equações Diofantinas elementares, destacadas dentre essas as equações de Pitágoras e de Pell, para as quais caracterizamos todas as soluções. Também apresentamos ao leitor o *método da descida de Fermat*, o qual fornece uma ferramenta por vezes útil para mostrar que certas equações Diofantinas não possuem soluções não triviais, num sentido a ser precisado.

2.1 Ternos Pitagóricos

Vamos começar estudando as soluções, em inteiros não nulos x, y e z, da equação $x^2+y^2 = z^2$, conhecida como a **equação de Pitágoras**. Após encontrá-las, veremos como utilizar as informações obtidas para resolver outras equações em números inteiros. O resultado fundamental está contido na seguinte

Figura 2.1: Pierre Simon de Fermat foi um funcionário público francês e matemático amador que viveu no século XVII e que teve a Matemática, notadamente a teoria dos números, como sua maior paixão.

Proposição 2.1. Os ternos (x, y, z) de inteiros não nulos tais que $x^2 + y^2 = z^2$ são dados por:

$$\begin{cases} x = 2uvd \\ y = (u^2 - v^2)d \\ z = (u^2 + v^2)d \end{cases} \quad \text{ou} \quad \begin{cases} x = (u^2 - v^2)d \\ y = 2uvd \\ z = (u^2 + v^2)d, \end{cases} \tag{2.1}$$

onde d, u e v são inteiros não nulos, com u e v de paridades distintas e primos entre si.

Prova. Sem perda de generalidade, podemos supor $x, y, z > 0$. Se $d = \text{mdc}\,(x, y)$, então $d^2 \mid (x^2 + y^2)$, i.e., $d^2 \mid z^2$; logo, $d \mid z$. Existem, portanto, inteiros não nulos a, b e c tais que $\text{mdc}\,(a, b) = 1$ e $(x, y, z) = (da, db, dc)$. Ademais, como

$$x^2 + y^2 = z^2 \Leftrightarrow a^2 + b^2 = c^2,$$

basta encontrarmos as soluções inteiras não nulas a, b e c da equação acima, sujeitas à condição $\text{mdc}\,(a, b) = 1$.

As condições $a^2 + b^2 = c^2$ e $\text{mdc}\,(a, b) = 1$ nos dão facilmente $\text{mdc}\,(a, c) = \text{mdc}\,(b, c) = 1$. Lembre agora (cf. corolário 1.8) que o quadrado de um inteiro t deixa resto 0 ou 1 quando dividido por 4, conforme t seja respectivamente par ou ímpar. Portanto, se a e b forem ímpares, então $c^2 = a^2 + b^2$ deixará resto 2 quando dividido por 4, uma contradição.

Como $\text{mdc}\,(a, b) = 1$, restam dois casos a considerar: a ímpar e b par ou vice-versa. Analisemos o primeiro deles, sendo a análise do segundo totalmente análoga. Sendo a ímpar e b par, segue de $c^2 = a^2 + b^2$ que c também é ímpar. Escreva, agora,

$$b^2 = (c - a)(c + a); \tag{2.2}$$

se $d' = \text{mdc}\,(c - a, c + a)$, então d' divide

$$(c + a) + (c - a) = 2c \quad \text{e} \quad (c + a) - (c - a) = 2a$$

e, daí, $d' \mid \text{mdc}\,(2a, 2c) = 2$. Mas, como $c - a$ e $c + a$ são ambos pares, segue que $d' = 2$ e podemos escrever (2.2) como

$$\left(\frac{b}{2}\right)^2 = \left(\frac{c - a}{2}\right)\left(\frac{c + a}{2}\right),$$

com $\text{mdc}\,\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = 1$. Segue do item (b) do corolário 1.22 a existência de naturais primos entre si u e v tais que $c + a = 2u^2$ e $c - a = 2v^2$, de forma que

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2.$$

Ademais, como $c = u^2 + v^2$ é ímpar, u e v têm paridades distintas.

Finalmente, por substituição na equação original, concluímos que os ternos acima são realmente soluções da equação, de modo que nada mais há a fazer. ■

Um terno (x, y, z) de inteiros positivos tais que $x^2 + y^2 = z^2$ é um **terno Pitagórico**, em alusão ao matemático grego Pitágoras de Samos e seu famoso teorema sobre triângulos retângulos. De fato, um

tal terno (x, y, z) determina um triângulo retângulo de catetos x e y e hipotenusa z.

Vejamos como aplicar o resultado acima para encontrar as soluções inteiras de outra equação diofantina.

Exemplo 2.2. Ache todas as soluções inteiras não nulas da equação $x^2 + y^2 = 2z^2$, com $x \neq \pm y$.

Solução. Em uma qualquer dessas soluções, devemos ter x e y ambos pares ou ambos ímpares, pois, caso contrário, $x^2 + y^2$ seria ímpar. Assim, tomando $a = \frac{x+y}{2}$ e $b = \frac{x-y}{2}$, temos $a, b \in \mathbb{Z} \setminus \{0\}$ e $x = a + b$, $y = a - b$. Substituindo tais expressões para x e y na equação original, concluímos que

$$x^2 + y^2 = 2z^2 \Leftrightarrow a^2 + b^2 = z^2.$$

Mas, uma vez que essa última equação é a equação de pitágoras, segue da proposição anterior a existência de inteiros não nulos d, u e v, com u e v primos entre si e de paridades distintas, tais que

$$a = 2uvd, \quad b = (u^2 - v^2)d, \quad z = (u^2 + v^2)d$$

ou

$$a = (u^2 - v^2)d, \quad b = 2uvd, \quad z = (u^2 + v^2)d.$$

Portanto, as soluções (x, y, z) da equação original, com $x \neq \pm y$, são de um dos tipos abaixo, onde d, u, v satisfazem as condições acima descritas:

$$x = (u^2 - v^2 + 2uv)d, \quad y = (-u^2 + v^2 + 2uv)d, \quad z = (u^2 + v^2)d$$

ou

$$x = (u^2 - v^2 + 2uv)d, \quad y = (u^2 - v^2 - 2uv)d, \quad z = (u^2 + v^2)d.$$

■

As equações analisadas acima são, em um certo sentido, privilegiadas, uma vez que possuem uma infinidade de soluções inteiras não nulas. Nosso próximo exemplo será o de uma equação que só admite a solução inteira $x = y = z = 0$; a prova que apresentaremos ilustra um método (a **descida de Fermat**) que pode, por vezes, ser utilizado a fim de provar que uma equação Diofantina não possui soluções inteiras não nulas.

Esquematicamente, o método da descida de Fermat consiste no cumprimento das seguintes etapas:

i. Supor que uma dada equação possui uma solução em inteiros não nulos.

ii. Concluir, a partir daí, que ela possui uma solução em inteiros não nulos que seja, em algum sentido, mínima.

iii. Deduzir a existência de uma solução em inteiros não nulos *menor* que a mínima (no sentido do item ii.), chegando, assim, a uma contradição.

Exemplo 2.3. Prove que a equação $3x^2+y^2 = 2z^2$ não possui soluções inteiras não nulas.

Prova. Inicialmente, observe que não podemos ter exatamente um dos inteiros x, y, z igual a 0. Suponha, pois, que a equação dada possua uma solução (x, y, z) com $x, y, z \in \mathbb{N}$ (uma vez que, se (x, y, z) for solução, então $(\pm x, \pm y, \pm z)$ também o será). Então, dentre todas tais soluções (x, y, z), existe uma para a qual z é o menor possível, digamos $x = a, y = b, z = c$. Trabalhemos tal solução.

Se $3 \nmid b$, temos de $3a^2 + b^2 = 2c^2$ que $3 \nmid c$. Mas aí, o corolário 1.8 garante que b^2 e c^2 deixam resto 1 na divisão por 3 e a igualdade $3a^2 + b^2 = 2c^2$ nos dá uma contradição. Logo, $3 \mid b$, digamos $b = 3b_1$ para algum $b_1 \in \mathbb{N}$, e segue de

$$2c^2 = 3a^2 + b^2 = 3(a^2 + 3b_1^2)$$

que $3 \mid c$. Sendo $c = 3c_1$, para algum $c_1 \in \mathbb{N}$, a igualdade acima nos dá

$$6c_1^2 = a^2 + 3b_1^2,$$

de modo que $3 \mid a$, digamos $a = 3a_1$, com $a_1 \in \mathbb{N}$. Portanto, a última igualdade acima fornece

$$2c_1^2 = 3a_1^2 + b_1^2,$$

de sorte que (a_1, b_1, c_1) é outra solução da equação original no conjunto dos números naturais. Contudo, a relação $0 < c_1 = \frac{c}{3} < c$ é uma contradição, uma vez que partimos de uma solução em naturais (a, b, c) para a qual c era o menor possível. Logo, nossa equação não possui soluções não nulas. ■

Voltando à equação de Pitágoras, uma generalização natural da mesma seria estudar a equação Diofantina mais geral abaixo, denominada **equação de Fermat**, onde $n > 2$ é um inteiro fixado:

$$x^n + y^n = z^n. \tag{2.3}$$

Por cerca de três séculos, muitos dos mais eminentes matemáticos defrontaram-se com o problema de decidir sobre a existência de soluções, em inteiros não nulos x, y, z, para essa equação. O próprio Fermat acreditava haver conseguido provar, provavelmente utilizando seu método da descida, que tal equação não possui soluções não nulas quando $n > 2$, e desde então esse resultado passou a ser conhecido como o **grande teorema de Fermat**. Entretanto, seu argumento nunca foi explicitamente escrito e, muito provavelmente, estava errado.

Na última década do século XX, o matemático inglês Andrew Wiles, com a colaboração do também inglês Richard Taylor e apoiando-se em importantes trabalhos anteriores de vários matemáticos, provou que a equação de Fermat não possui soluções em inteiros não nulos

x, y, z quando $n > 2$, utilizando, para tanto, matemática muitíssimo avançada[1].

Podemos, entretanto, aproveitar o método da descida para analisar um caso simples da equação (2.3), aquele em que $4 \mid n$.

Exemplo 2.4. Se n for um natural múltiplo de 4, então não existem inteiros não nulos x, y, z tais que $x^n + y^n = z^n$.

Prova. Seja $n = 4k$, com k natural. De $x^n + y^n = z^n$, obtemos

$$(x^k)^4 + (y^k)^4 = (z^{2k})^2,$$

ou seja, (x^k, y^k, z^{2k}) é solução não nula da equação $a^4 + b^4 = c^2$. Assim, basta mostrarmos que essa última equação não admite soluções em inteiros não nulos.

Por absurdo, suponhamos que existam $a, b, c \in \mathbb{N}$ tais que $a^4 + b^4 = c^2$. Podemos também supor que a, b, c foram escolhidos de tal modo que não haja outra solução positiva (α, β, γ) com $\gamma < c$ (esta é a hipótese que vamos usar no método da descida). Como (a^2, b^2, c) resolve a equação de Pitágoras, a proposição 2.1, juntamente com a minimalidade de c, garante que $\text{mdc}\,(a^2, b^2) = 1$ e que existem naturais u e v, primos entre si e de paridades distintas, tais que

$$a^2 = u^2 - v^2, \quad b^2 = 2uv, \quad c = u^2 + v^2$$

ou

$$a^2 = 2uv, \quad b^2 = u^2 - v^2, \quad c = u^2 + v^2.$$

Analisemos o primeiro caso acima, sendo a análise do segundo totalmente análoga. Então, a é ímpar e, como $a^2 + v^2 = u^2$, segue

[1] Veja também [9], onde é apresentado um relato *romanceado* super interessante da saga de Andrew Wiles e de outros matemáticos na busca de uma prova para o grande teorema de Fermat.

novamente da caracterização dos ternos pitagóricos a existência de naturais p e q, primos entre si e de paridades distintas, tais que

$$a = p^2 - q^2, \quad v = 2pq, \quad u = p^2 + q^2.$$

Mas aí,

$$b^2 = 2uv = 4pq(p^2 + q^2)$$

e, como mdc $(p, q) = 1$, temos que ambos p e q são também primos com $p^2 + q^2$. Portanto, a fim de que $4pq(p^2 + q^2)$ seja um quadrado perfeito, devemos ter p, q e $p^2 + q^2$ quadrados perfeitos, digamos

$$p = \alpha^2, \quad q = \beta^2, \quad p^2 + q^2 = \gamma^2,$$

com $\alpha, \beta, \gamma \in \mathbb{N}$. Segue, então, que

$$\alpha^4 + \beta^4 = p^2 + q^2 = \gamma^2,$$

com

$$c = u^2 + v^2 > u = p^2 + q^2 = \gamma^2 \geq \gamma,$$

contrariando a minimalidade de c. Logo, não há soluções não nulas de $x^n + y^n = z^n$ quando $4 \mid n$. ∎

Terminamos esta seção apresentando um exemplo de uso bem mais elaborado do método de descida.

Exemplo 2.5 (IMO). Sejam a, b, c, d inteiros tais que $a > b > c > d > 0$. Suponha que

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove que $ab + cd$ nunca é um número primo.

Prova. Simplificando a condição do enunciado obtemos $a^2 + c^2 - ac = b^2 + d^2 + bd$ ou, ainda,

$$(2a - c)^2 + 3c^2 = (b + 2d)^2 + 3b^2. \tag{2.4}$$

Suponha, por contradição, que $ab + cd = p$, p primo. A condição $a > b > c > d > 0$ garante que $p = ab + cd \geq 4 \cdot 3 + 2 \cdot 1 = 14$, de modo que $p \geq 17$. Por outro lado,

$$2p = 2ab + 2cd = (2a - c)b + (b + 2d)c,$$

de modo que mdc $(2a - c, b + 2d)$ divide $2p$. Para *mdc* $(2a - c, b + 2d)$ ser par deveríamos ter b e c pares, donde $p = ab + cd$ seria par, o que é um absurdo. Logo,

$$\text{mdc}\,(2a - c, b + 2d) = 1 \quad \text{ou} \quad p.$$

Afirmamos que mdc $(2a - c, b + 2d) = 1$. Suponha que mdc $(2a - c, b + 2d) = p$. Então (2.4) nos daria que $p^2 \mid 3(b^2 - c^2)$ e, daí, $p^2 \mid (b^2 - c^2)$, uma vez que $p \neq 3$. Porém, $p = ab + cd > b$, de modo que $0 < b^2 - c^2 < p^2$, um absurdo.

Agora, sejam $x = 2a - c$, $y = b + 2d$. Então mdc $(x, y) = 1$ e segue de (2.4) que $x^2 - y^2 = 3(b^2 - c^2)$ ou, ainda,

$$(x - y)(x + y) = 3(b - c)(b + c).$$

Consideraremos dois casos separadamente:

(a) b e c têm paridades distintas: o fato de ser $p = ab + cd$ garante que *mdc* $(b, c) = 1$. Como $b + c$ e $b - c$ são ímpares, isto implica em mdc $(b + c, b - c) = 1$. Um argumento análogo implica em mdc $(x + y, x - y) = 1$ também. Se $3 \mid (x + y)$ então

$$x - y = \text{mdc}\,(x - y, (b + c)(b - c)) = \text{mdc}\,(x - y, b + c)\,\text{mdc}\,(x - y, b - c)$$

e

$$x + y = 3\,\text{mdc}\,(x + y, (b + c)(b - c)) = 3\,\text{mdc}\,(x + y, b + c)\,\text{mdc}\,(x + y, b - c).$$

Escrevendo $\alpha = \text{mdc}\,(x-y, b-c)$, $\beta = \text{mdc}\,(x-y, b+c)$, $\gamma = \text{mdc}\,(x+y, b-c)$ e $\delta = \text{mdc}\,(x+y, b+c)$, obtemos $x - y = \alpha\beta$ e $x + y = 3\gamma\delta$. Por outro lado,

$$b - c = \text{mdc}\,(b-c, x-y)\,\text{mdc}\,(b-c, x+y) = \alpha\gamma$$

e, analogamente, $b + c = \beta\delta$. Resolvendo para a, b, c, d obtemos

$$4a = \alpha\beta + \beta\delta + 3\gamma\delta - \alpha\gamma, \quad 2b = \alpha\gamma + \beta\delta,$$

$$2c = -\alpha\gamma + \beta\delta \quad \text{e} \quad 4d = -\alpha\beta - \beta\delta + 3\gamma\delta - \alpha\gamma.$$

Daí

$$8p = 8(ab + cd) = \beta\delta(2\alpha^2 + 3\delta^2).$$

Mas, como $b + c$ ímpar, temos β e δ são ímpares e, portanto, $\beta\delta(2\alpha^2 + 3\delta^2)$ é ímpar, o que é um absurdo. Se $3 \mid (x - y)$ chegamos a uma contradição de modo análogo.

(b) b e c têm paridades iguais: nesse caso, b e c devem ser ímpares, pois, do contrário, 2 dividiria $ab + cd = p$. Assim, nas notações acima, temos x e y também ímpares. Segue que

$$\text{mdc}\,(b+c, b-c) = \text{mdc}\,(x+y, x-y) = 2,$$

pois já temos $\text{mdc}\,(x, y) = 1$. Se $3 \mid (x+y)$ (o outro caso é novamente análogo), escrevendo

$$\left(\frac{x-y}{2}\right)\left(\frac{x+y}{2}\right) = 3\left(\frac{b-c}{2}\right)\left(\frac{b+c}{2}\right)$$

e pondo

$$\alpha = \text{mdc}\left(\frac{x-y}{2}, \frac{b-c}{2}\right), \quad \beta = \text{mdc}\left(\frac{x-y}{2}, \frac{b+c}{2}\right),$$

$$\gamma = \text{mdc}\left(\frac{x+y}{2}, \frac{b-c}{2}\right), \quad \delta = \text{mdc}\left(\frac{x+y}{2}, \frac{b+c}{2}\right)$$

chegamos, como acima, a $2a = \alpha\beta + \beta\delta + 3\gamma\delta - \alpha\gamma$, $b = \alpha\gamma + \beta\delta$, $c = -\alpha\gamma + \beta\delta$ e $2d = -\alpha\beta - \beta\delta + 3\gamma\delta - \alpha\gamma$. Daí,

$$2p = 2(ab + cd) = \beta\delta(2\alpha^2 + 3\delta^2).$$

Nem β nem δ são iguais a p, pois, do contrário, teríamos $b > p$, o que contradiz ser $ab + cd = p$. Logo $\beta\delta \leq 2$, donde $0 < d < c \leq 2 - \alpha\gamma \leq 1$, um absurdo. ■

Problemas – Seção 2.1

1. (OBM - adaptado.) Dados $n, k \in \mathbb{N}$, prove que a equação $x^n + ky^n = z^{n+1}$ possui infinitas soluções em inteiros positivos x, y, z.

2. Encontre todas as soluções, em inteiros positivos, da equação

$$(x + y)^2 + (y + z)^2 = (x + z)^2.$$

3. Mostre que as soluções em inteiros não nulos da equação $x^2 + 2y^2 = z^2$ são dadas por

$$x = \pm(u^2 - 2v^2)d, \quad y = \pm 2uvd, \quad z = \pm(u^2 + 2v^2)d,$$

onde d, u e v são inteiros não nulos, com u e $2v$ primos entre si.

4. Mostre que nenhuma das equações a seguir possui soluções inteiras não nulas:

   (a) $x^4 + 4y^4 = z^2$.
   (b) $x^4 + 2y^4 = z^2$.
   (c) $x^2 + y^2 = 3z^2$.
   (d) $x^3 + 5y^3 = 9z^3$.

5. (a) (Hungria.) Mostre que não existem soluções racionais x e y para a equação $x^2 + xy + y^2 = 2$.

   (b) Encontre todas as soluções racionais x e y para a equação $x^2 + xy + y^2 = 1$.

6. Prove o seguinte teorema de Euler: não existem inteiros não nulos w, x, y e z tais que $w^2 + x^2 + y^2 = 7z^2$.

7. (Bulgária.) Prove que não existem x, y e z racionais, tais que

$$x^2 + y^2 + z^2 + 3(x + y + z) + 5 = 0.$$

8. (Crux.) Seja r um inteiro positivo dado. Queremos calcular o número de triângulos retângulos ABC, dois a dois não congruentes, satisfazendo as condições a seguir:

   (a) O raio do círculo inscrito em ABC mede r.

   (b) Os comprimentos dos lados de ABC são números inteiros primos entre si.

   Mostre que o número de tais triângulos é 2^k, onde k é o número de fatores primos distintos de r.

9. (IMO.) Dados $n \in \mathbb{N}$ e um círculo de raio 1, mostre que podemos escolher n pontos $A_1, A_2, \ldots, A_n$ sobre o mesmo, tais que A_iA_j é racional, quaisquer que sejam $1 \leq i < j \leq n$.

2.2 A equação de Pell

Examinamos, nesta seção, as soluções de equações do tipo

$$x^2 - dy^2 = m, \tag{2.5}$$

onde $d > 1$ é um inteiro livre de quadrados (cf. problema 6, página 47) e m é um inteiro qualquer. A equação acima é conhecida como a **equação de Pell**[2].

Uma vez que d é um produto de primos distintos, o exemplo 1.23 garante que $\sqrt{d}$ é irracional. Em particular, quando $m = 0$ a equação acima não admite soluções inteiras além da trivial $x = y = 0$, pois, se não fosse este o caso, teríamos $x, y \neq 0$ e, daí, $\sqrt{d} = \frac{x}{y} \in \mathbb{Q}$. Por outro lado, se $d, m < 0$, então a equação de Pell não tem soluções e, se $d < 0 < m$, então (2.5) tem no máximo um número finito de soluções. No entanto, mesmo para $d, m > 0$, (2.5) pode não ter nenhuma solução, conforme atesta o problema 1.

Doravante, suporemos que $m = 1$ (o caso geral é parcialmente respondido pelo problema 5; a esse respeito, veja também [5]). O exemplo a seguir mostra, nesse caso, que (2.5) pode ter uma infinidade de soluções.

Exemplo 2.6. A equação $x^2 - 2y^2 = 1$ possui uma infinidade de soluções inteiras positivas.

Prova. Note que $x = 3$, $y = 2$ é uma solução. Por outro lado, podemos gerar infinitas soluções dessa equação a partir de uma solução não nula (a, b), do seguinte modo: partindo de $a^2 - 2b^2 = 1$, temos

$$(a + b\sqrt{2})(a - b\sqrt{2}) = 1$$

e, daí,

$$(a + b\sqrt{2})^2(a - b\sqrt{2})^2 = 1.$$

Desenvolvendo os binômios, chegamos a

$$(a^2 + 2b^2 + 2ab\sqrt{2})(a^2 + 2b^2 - 2ab\sqrt{2}) = 1$$

ou, ainda, a

$$(a^2 + 2b^2)^2 - 2(2ab)^2 = 1.$$

[2]Após John Pell, matemático inglês do século XVII.

Portanto, $(a^2+2b^2, 2ab)$ também será solução e, sendo a e b naturais, temos $a < a^2+2b^2$. Repetindo o argumento acima sucessivas vezes, obtemos uma infinidade de soluções para a equação dada. ■

O método utilizado no exemplo acima se generaliza facilmente para mostrar que a equação de Pell $x^2-dy^2=1$ admite infinitas soluções não nulas, desde que admita pelo menos uma tal solução; ademais, com poucas modificações podemos tratar equações mais gerais (cf. problemas 5 e 7, por exemplo).

Apesar de, em certos casos particulares, podermos encontrar facilmente infinitas soluções da equação (2.5), por enquanto não sabemos se há outras. A fim de responder essa pergunta, precisamos de um resultado preliminar sobre aproximação de irracionais por racionais, devido a G. L. Dirichlet. Para a prova do mesmo, lembre-se de que (cf. dicussão que precede o problema 15, página 32), para $x \in \mathbb{R}$, a **parte fracionária** de x é o número real $\{x\} \in [0,1)$, definido por $\{x\} = x - \lfloor x \rfloor$.

Lema 2.7 (Dirichlet). Se α é um irracional qualquer, então existem infinitos racionais $\frac{x}{y}$, com x e y inteiros não nulos, primos entre si e tais que

$$\left|\frac{x}{y}-\alpha\right| < \frac{1}{y^2}.$$

Prova. Seja $n > 1$ um inteiro qualquer e considere os $n+1$ números $\{j\alpha\} \in [0,1)$, com $j = 0, 1, \ldots, n$. Como

$$[0,1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \cdots \cup \left[\frac{n-1}{n}, 1\right),$$

uma união de n conjuntos, o princípio da casa dos pombos garante a existência de índices $0 \le k < j \le n$ tais que $\{j\alpha\}$ e $\{k\alpha\}$ pertencem a um mesmo intervalo dos que aparecem no lado direito da igualdade acima. Então $|\{j\alpha\}-\{k\alpha\}| < \frac{1}{n}$ ou, o que é o mesmo,

$$|(j-k)\alpha - (\lfloor j\alpha \rfloor - \lfloor k\alpha \rfloor)| < \frac{1}{n}.$$

Segue, daí, que

$$\left|\alpha - \frac{\lfloor j\alpha \rfloor - \lfloor k\alpha \rfloor}{j-k}\right| < \frac{1}{(j-k)n} \le \frac{1}{(j-k)^2}, \tag{2.6}$$

e fazendo $x = \lfloor j\alpha \rfloor - \lfloor k\alpha \rfloor$ e $y = j-k$, temos $0 < y \le n$ e $\left|\frac{x}{y}-\alpha\right| < \frac{1}{y^2}$. Por outro lado, se $d = \text{mdc}\,(x,y)$ e $x = dx_1, y = dy_1$, então

$$\left|\frac{x_1}{y_1}-\alpha\right| < \frac{1}{y^2} \le \frac{1}{y_1^2},$$

de modo que podemos supor que $\text{mdc}\,(x,y)=1$.

Para garantirmos a existência de infinitos tais pares, sejam x e y inteiros não nulos, primos entre si e tais que $\left|\frac{x}{y}-\alpha\right| < \frac{1}{y^2}$. Escolhendo um natural n_1 tal que $\left|\frac{x}{y}-\alpha\right| > \frac{1}{n_1}$ e repetindo (com n_1 no lugar de n) o argumento que levou a (2.6), obtemos inteiros não nulos e primos entre si x_1 e y_1, tais que $0 < y_1 \le n_1$ e

$$\left|\frac{x_1}{y_1}-\alpha\right| < \frac{1}{n_1y_1} \le \frac{1}{y_1^2}.$$

Por outro lado,

$$\left|\frac{x_1}{y_1}-\alpha\right| < \frac{1}{n_1y_1} \le \frac{1}{n_1} < \left|\frac{x}{y}-\alpha\right|,$$

de sorte que $\frac{x_1}{y_1} \ne \frac{x}{y}$. Repetindo esse argumento sucessivas vezes, obtemos uma infinidade de pares (x,y) com as propriedades desejadas. ■

O lema de Dirichlet permite mostrar que, fixado um natural d livre de quadrados, a equação (2.5) admite uma infinidade de soluções para pelo menos um valor inteiro de m.

Lema 2.8. Se $d > 1$ é um natural livre de quadrados, então existe $m \in \mathbb{Z} \setminus \{0\}$ tal que a equação $x^2-dy^2=m$ admite infinitas soluções inteiras.

Prova. Como $\sqrt{d} \notin \mathbb{Q}$, o lema de Dirichlet garante que o conjunto S dos pares (x, y) de inteiros não nulos, primos entre si e tais que $\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{y^2}$ é infinito. Mas, se (x, y) for um tal par ordenado, então $|x - y\sqrt{d}| < \frac{1}{|y|}$ e a desigualdade triangular nos dá

$$\begin{aligned}|x^2 - dy^2| &= |x - y\sqrt{d}||x + y\sqrt{d}| < \frac{1}{|y|}\left(|x - y\sqrt{d}| + 2|y|\sqrt{d}\right)\\ &= \frac{1}{|y|}\left(\frac{1}{|y|} + 2|y|\sqrt{d}\right) < 2\sqrt{d} + 1.\end{aligned}$$

De outro modo, para $(x, y) \in S$, o conjunto dos inteiros $x^2 - dy^2$ está contido no conjunto dos inteiros não nulos situados entre os números reais $-(2\sqrt{d} + 1)$ e $2\sqrt{d} + 1$. Mas, uma vez que tal conjunto é finito, existe um inteiro $m \neq 0$ entre $-(2\sqrt{d} + 1)$ e $2\sqrt{d} + 1$, o qual se repete um número infinito de vezes dentre os valores de $x^2 - dy^2$, para $(x, y) \in S$. Por fim, isso é o mesmo que dizer que a equação $x^2 - dy^2 = m$ admite uma infinidade de soluções inteiras. ■

Estamos finalmente em condições de caracterizar todas as soluções de (2.5) quando $m = 1$; os ingredientes-chave serão o lema anterior e o método da descida de Fermat.

Proposição 2.9. Se $d > 1$ é um natural livre de quadrados, então a equação $x^2 - dy^2 = 1$ admite pelo menos uma solução em inteiros positivos x, y.

Prova. Tome, pelo lema anterior, $m \in \mathbb{Z} \setminus \{0\}$ tal que a equação $x^2 - dy^2 = m$ tenha uma infinidade de soluções. Como os restos da divisão de um inteiro por m são em número finito, podemos escolher duas dessas soluções, (x_1, y_1) e (x_2, y_2) digamos, tais que $|x_1| \neq |x_2|$ e m divida $x_2 - x_1, y_2 - y_1$. Então

$$(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = (x_1x_2 - dy_1y_2) + (x_2y_1 - x_1y_2)\sqrt{d} \quad (2.7)$$

e, se $x_2 - x_1 = mr$ e $y_2 - y_1 = ms$, com $r, s \in \mathbb{Z}$, temos

$$\begin{aligned}x_1x_2 - dy_1y_2 &= x_1(x_2 - x_1) + (x_1^2 - dy_1^2) + (y_1 - y_2)dy_1\\ &= m(rx_1 + 1 - sdy_1)\end{aligned}$$

e

$$x_2y_1 - x_1y_2 = (x_2 - x_1)y_1 + x_1(y_1 - y_2) = m(r - s).$$

Por simplicidade de notação, escrevamos $x_1x_2 - dy_1y_2 = mu$ e $x_2y_1 - x_1y_2 = mv$, com $u, v \in \mathbb{Z}$. Segue de (2.7) que

$$(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = m(u + v\sqrt{d}) \quad (2.8)$$

e, daí,

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = m(u - v\sqrt{d}).$$

Multiplicando ordenadamente essas duas igualdades, chegamos a

$$m^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = m^2(u^2 - dv^2),$$

de maneira que $u^2 - dv^2 = 1$.

Resta mostrar que $u, v \neq 0$. Se $u = 0$, teríamos $-dv^2 = 1$, claramente um absurdo. Se $v = 0$, teríamos $u = \pm 1$ e seguiria de (2.8) que

$$(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = \pm m = \pm(x_2^2 - dy_2^2);$$

logo,

$$x_1 + y_1\sqrt{d} = \pm(x_2 + y_2\sqrt{d})$$

e, daí, $|x_1| = |x_2|$, uma vez que $\sqrt{d} \notin \mathbb{Q}$. Mas isso contradiz nossas escolhas de x_1 e x_2. ■

Chegamos finalmente ao resultado desejado, o qual caracteriza todas as soluções da equação $x^2 - dy^2 = 1$, quando $d > 1$ é um natural livre de quadrados. Observe que, pela proposição anterior, tal equação admite pelo menos uma solução.

Teorema 2.10. Se $d > 1$ é um natural livre de quadrados, então a equação $x^2 - dy^2 = 1$ admite infinitas soluções em inteiros positivos x e y. Mais precisamente, se $x = x_1$ e $y = y_1$ é a solução em inteiros positivos para a qual a soma $x + y\sqrt{d}$ é a menor possível, então as demais soluções inteiras positivas da equação são dadas pelos naturais x_n, y_n que satisfazem a igualdade

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,$$

onde n é um número natural.

Prova. Seja $\alpha = x_1 + y_1\sqrt{d}$, com $x_1, y_1 \in \mathbb{N}$ escolhidos como no enunciado.

Dado $n \in \mathbb{N}$, sabemos (cf. exemplo 6.11 do volume 1) que existem $x_n, y_n \in \mathbb{N}$ tais que

$$(x_1 \pm y_1\sqrt{d})^n = x_n \pm y_n\sqrt{d}.$$

Assim,

$$\begin{aligned} 1 &= (x_1^2 - dy_1^2)^n = (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n \\ &= (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = x_n^2 - dy_n^2, \end{aligned}$$

de modo que todos os pares (x_n, y_n) do enunciado são soluções da equação.

Agora, se (x, y) é uma solução qualquer em inteiros positivos, basta mostrarmos que existe $n \in \mathbb{N}$ tal que

$$x + y\sqrt{d} = \alpha^n.$$

Suponha o contrário. Como $\alpha > 1$, temos $\lim_{n\to+\infty} \alpha^n = +\infty$, de sorte que existe $n \in \mathbb{N}$ tal que

$$\alpha^n < x + y\sqrt{d} < \alpha^{n+1}$$

ou, ainda,

$$1 < \frac{x + y\sqrt{d}}{\alpha^n} < \alpha. \tag{2.9}$$

Mas, como $\alpha^n = x_n + y_n\sqrt{d}$ e $x_n^2 - dy_n^2 = 1$, seguiria então que

$$\begin{aligned} \frac{x + y\sqrt{d}}{\alpha^n} &= \frac{x + y\sqrt{d}}{x_n + y_n\sqrt{d}} \\ &= (x_n - y_n\sqrt{d})(x + y\sqrt{d}) \\ &= (xx_n - dyy_n) + (x_ny - y_nx)\sqrt{d}, \end{aligned}$$

com

$$(xx_n - dyy_n)^2 - d(x_ny - y_nx)^2 = (x_n^2 - dy_n^2)(x^2 - dy^2) = 1.$$

Portanto, $(xx_n - dyy_n, x_ny - y_nx)$ também é solução, tal que (por (2.9))

$$1 < (xx_n - dyy_n) + (x_ny - y_nx)\sqrt{d} = \frac{x + y\sqrt{d}}{\alpha^n} < \alpha.$$

Assim, se mostrarmos que $xx_n - dyy_n, x_ny - y_nx > 0$, obteremos uma contradição à minimalidade de α (observe que, aqui, operamos com a descida de Fermat).

Para o que falta, sendo

$$a = xx_n - dyy_n \quad \text{e} \quad b = x_ny - y_nx,$$

temos $a + b\sqrt{d} = \frac{x+y\sqrt{d}}{\alpha^n} > 1$ e $a^2 - db^2 = 1$, de modo que

$$a - b\sqrt{d} = \frac{1}{a + b\sqrt{d}} > 0.$$

Então, por um lado,

$$2a = (a - b\sqrt{d}) + (a + b\sqrt{d}) > 0;$$

por outro,

$$a - b\sqrt{d} = \frac{1}{a + b\sqrt{d}} < 1$$

nos dá $b\sqrt{d} > a - 1 \geq 0$, de sorte que $b > 0$. ■

Exemplo 2.11. Ache todas as soluções da equação $x^2 - 2y^2 = 1$ em naturais x e y.

Solução. O teorema anterior ensina que as soluções inteiras positivas dessa equação são da forma (x_n, y_n), onde x_n e y_n são os únicos inteiros positivos para os quais

$$x_n + y_n\sqrt{2} = (x_1 + y_1\sqrt{2})^n,$$

e (x_1, y_1) é a solução positiva tal que $x_1 + y_1\sqrt{2}$ é o menor possível. Como os pares $(1,1)$, $(1,2)$, $(2,1)$, $(2,2)$, $(3,1)$, $(1,3)$, $(2,3)$ e $(4,1)$ não são soluções da equação mas $(3,2)$ o é, é imediato verificar que $x_1 = 3, y_1 = 2$. Portanto, as soluções positivas são os pares (x_n, y_n) dados pela igualdade

$$x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n.$$

■

Problemas – Seção 2.2

1. * Se d e m deixam resto 3 quando divididos por 4, mostre que a equação (2.5) não possui soluções inteiras.

2. Em relação ao exemplo 2.11, prove que as soluções inteiras positivas (x_n, y_n) da equação $x^2 - 2y^2 = 1$ são definidas recursivamente por $x_1 = 3$, $y_1 = 2$ e, para $n \geq 1$ inteiro,

$$x_{n+1} = 3x_n + 4y_n, \text{ e } y_{n+1} = 2x_n + 3y_n.$$

3. Prove, sem usar o teorema 2.10, que a equação $x^2 - 2y^2 = -1$ admite uma infinidade de soluções inteiras.

4. Mostre que há infinitos inteiros positivos n tais que $n^2 + (n+1)^2$ é um quadrado perfeito.

5. * Sejam $d, m \in \mathbb{N}$, sendo $d > 1$ livre de quadrados. Se a equação $x^2 - dy^2 = m$ tiver uma solução (x_0, y_0) em inteiros positivos, prove que ela terá infinitas soluções.

6. Ache uma infinidade de soluções inteiras positivas para a equação

$$y^2 + 1 = x(x + y).$$

7. Generalize o problema anterior do seguinte modo: sejam $a, b, c \in \mathbb{Z}$ tais que $\Delta = b^2 - 4ac$ é maior que 1 e livre de quadrados. Se $n \in \mathbb{Z}$ for tal que a equação

$$x^2 - \Delta y^2 = 4an$$

tem ao menos uma solução inteira (x_0, y_0), tal que $2a \mid (x_0 - by_0)$, mostre que a equação

$$ax^2 + bxy + cy^2 = n$$

tem infinitas soluções inteiras.

CAPÍTULO 3

Funções Aritméticas Multiplicativas

Este breve capítulo introduz uma importante classe de funções, ditas *aritméticas multiplicativas*, as quais desempenham papel de relevo na teoria elementar dos números. Dentre as muitas funções aritméticas multiplicativas que estudaremos, duas destacam-se, de nosso ponto de vista: a função de Möbius, essencial à obtenção da célebre *fórmula de inversão de Möbius*, e a função φ de Euler, que se revelará imprescindível para os desenvolvimentos teóricos constantes dos capítulos subsequentes.

Em tudo o que segue, nos referiremos a uma função $f : \mathbb{N} \to \mathbb{R}$ como uma **função aritmética**.

Definição 3.1. Uma função aritmética $f : \mathbb{N} \to \mathbb{R}$ é **multiplicativa** se, para todos $m, n \in \mathbb{N}$ primos entre si, tivermos $f(mn) = f(m)f(n)$.

Como 1 é relativamente primo consigo mesmo, segue que, se $f : \mathbb{N} \to \mathbb{R}$ for uma função aritmética multiplicativa, então $f(1) = f(1)^2$, de modo que $f(1) = 0$ ou 1. Caso seja $f(1) = 0$, teremos

$$f(n) = f(n \cdot 1) = f(n)f(1) = 0, \ \forall \ n \in \mathbb{N},$$

i.e., f será a função identicamente nula. Portanto, doravante suporemos, salvo menção explícita em contrário, que se $f : \mathbb{N} \to \mathbb{R}$ for uma função aritmética multiplicativa, então $f(1) = 1$.

Note ainda que, se $f : \mathbb{N} \to \mathbb{R}$ for uma função aritmética multiplicativa e $n > 1$ é um inteiro com decomposição canônica em primos da forma $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, então repetidas aplicações da definição nos dão

$$f(n) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k}). \tag{3.1}$$

Em palavras, a igualdade acima significa que, para sabermos calcular os valores $f(n)$, com $n \in \mathbb{N}$, é suficiente sabermos calcular os valores $f(p^\alpha)$, com p primo e $\alpha \in \mathbb{N}$.

Por fim, se $f : \mathbb{N} \to \mathbb{R}$ for uma função aritmética tal que $f(1) = 1$, então a relação $f(mn) = f(m)f(n)$ é sempre satisfeita quando $m = 1$ ou $n = 1$; portanto, para provarmos que uma tal f é multiplicativa, basta considerarmos o caso $m, n > 1$.

Utilizaremos várias vezes as observações acima sem maiores comentários.

Exemplo 3.2. Vimos no corolário 1.45 que, se $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ é a decomposição canônica de um natural $n > 1$ em primos, então

$$d(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$$

é o número de divisores positivos do natural n. Afirmamos que a função $d : \mathbb{N} \to \mathbb{R}$ assim obtida, denominada **função número de divisores positivos**, é multiplicativa. De fato, para $m, n > 1$ primos entre si, com decomposições canônicas em primos $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ e

$m = q_1^{\beta_1} \dots q_l^{\beta_l}$, temos $p_i \neq q_j$ para todos i, j. Portanto, a decomposição canônica de mn em primos é

$$mn = p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_l^{\beta_l}$$

e, daí,

$$d(mn) = (\alpha_1 + 1) \dots (\alpha_k + 1)(\beta_1 + 1) \dots (\beta_l + 1) = d(m)d(n).$$

No que segue, para $n \in \mathbb{N}$, denotaremos por $D(n)$ o conjunto dos divisores positivos de n, de sorte que $d(n) = |D(n)|$.

Lema 3.3. Se m e n são naturais primos entre si, então a aplicação

$$\begin{array}{rccc} f: & D(m) \times D(n) & \longrightarrow & D(mn) \\ & (x, y) & \longmapsto & xy \end{array}$$

é uma bijeção.

Prova. Segue do exemplo 3.2 e do princípio fundamental da contagem (cf. corolário 1.9 do volume 4) que

$$|D(mn)| = d(mn) = d(m)d(n) = |D(m)| \cdot |D(n)| = |D(m) \times D(n)|.$$

Portanto, o domínio e o contradomínio de f têm quantidades iguais de elementos, de modo que, para provarmos que f é uma bijeção, basta estabelecermos sua sobrejetividade. Para tanto, apliquemos o item (d) da proposição 1.21: se $k \mid mn$, então a condição $\text{mdc}\,(m, n) = 1$ garante que

$$k = \text{mdc}\,(k, mn) = \text{mdc}\,(k, m) \cdot \text{mdc}\,(k, n).$$

Portanto, fixado $k \in D(mn)$ e pondo $a = \text{mdc}\,(k, m)$ e $b = \text{mdc}\,(k, n)$, temos $a \in D(m)$, $b \in D(n)$ e $f((a, b)) = ab = k$, de sorte que k pertence à imagem de f. Mas, como $k \in D(mn)$ foi escolhido arbitrariamente, segue que f é sobrejetiva. ■

Em tudo o que segue, escreveremos $\sum_{0<d|n} f(d)$ para denotar o somatório dos valores $f(d)$ quando d varia em $D(n)$. A proposição a seguir estabelece uma das mais importantes propriedades das funções aritméticas multiplicativas.

Proposição 3.4. Se $f : \mathbb{N} \to \mathbb{R}$ é uma função aritmética multiplicativa, então a função $F : \mathbb{N} \to \mathbb{R}$ dada por

$$F(n) = \sum_{0<d|n} f(d)$$

também é multiplicativa.

Prova. Se $\mathrm{mdc}\,(m,n) = 1$, segue do lema anterior e do caráter multiplicativo de f que

$$\begin{aligned} F(mn) &= \sum_{0<d|mn} f(d) = \sum_{\substack{0<d_1|m \\ 0<d_2|n}} f(d_1 d_2) = \sum_{0<d_1|m} \sum_{0<d_2|n} f(d_1)f(d_2) \\ &= \left(\sum_{0<d_1|m} f(d_1)\right)\left(\sum_{0<d_2|n} f(d_2)\right) \\ &= F(m)F(n). \end{aligned}$$

■

Exemplo 3.5. A função $f : \mathbb{N} \to \mathbb{R}$ dada por $f(n) = n$ é obviamente multiplicativa. Portanto, segue da proposição anterior que a função $s : \mathbb{N} \to \mathbb{R}$ dada por

$$s(n) = \sum_{0<d|n} f(d) = \sum_{0<d|n} d$$

também é multiplicativa. A função s é a função **soma de divisores positivos**. Para $n = p^\alpha$, com p primo e $\alpha \in \mathbb{N}$, segue do corolário 1.45 que

$$s(p^\alpha) = \sum_{0<d|p^\alpha} d = \sum_{j=0}^{\alpha} p^j = \frac{p^{\alpha+1}-1}{p-1}.$$

Portanto, se $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, com $p_1 < \cdots < p_k$ primos e $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, segue de (3.1) e dos cálculos acima que

$$s(n) = \prod_{j=1}^{k} s(p_j^{\alpha_j}) = \prod_{j=1}^{k} \left(\frac{p_j^{\alpha_j+1}-1}{p_j-1}\right). \tag{3.2}$$

Para o exemplo a seguir, lembramos (cf. problema 6, página 47) que um inteiro $n > 1$ é *livre de quadrados* se $n = p_1 \ldots p_k$, com $p_1 < \cdots < p_k$ primos; equivalentemente, n é livre de quadrados se não existe um inteiro $q > 1$ tal que $q^2 \mid n$.

A próxima definição apresenta uma das mais importantes funções aritméticas multiplicativas, a *função de Möbius*.

Definição 3.6. A função de Möbius[1] é a função $\mu : \mathbb{N} \to \mathbb{R}$ dada por

$$\mu(n) = \begin{cases} 1, & \text{se } n = 1 \\ 0, & \text{se } q^2 \mid n, \text{ para algum inteiro } q > 1 \\ (-1)^k, & \text{se } n = p_1 \ldots p_k, \text{ com } p_1, \ldots, p_k \text{ primos distintos} \end{cases}.$$

Para verificar que a função de Möbius é multiplicativa, sejam $m, n > 1$ inteiros primos entre si. Então, mn será divisível por um quadrado maior que 1 se, e só se, m ou n o forem; sendo esse o caso, é imediato que

$$f(mn) = 0 = f(m)f(n).$$

Por outro lado, se m e n forem livres de quadrados, digamos $n = p_1 \ldots p_k$ e $m = q_1 \ldots q_l$, com $p_1 < \cdots < p_k$ e $q_1 < \cdots < q_l$ primos, a condição $\mathrm{mdc}\,(m,n) = 1$ garante que $p_i \neq q_j$ para todos i, j. Portanto, $mn = p_1 \ldots p_k q_1 \ldots q_l$ é a decomposição canônica de mn em primos, de sorte que

$$\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n).$$

[1] Após o matemático alemão do século XIX August Möbius.

A proposição a seguir destaca uma importante propriedade da função de Möbius.

Proposição 3.7. Se $\mu : \mathbb{N} \to \mathbb{R}$ é a função de Möbius, então

$$\sum_{0<d|n} \mu(d) = \begin{cases} 1, & \text{se } n = 1 \\ 0, & \text{se } n > 1 \end{cases}.$$

Prova. Seja $F : \mathbb{N} \to \mathbb{R}$ a função dada por

$$F(n) = \sum_{0<d|n} \mu(d).$$

Pela proposição 3.4, F é multiplicativa, e queremos mostrar que $F(1) = 1$ e $F(n) = 0$ para $n > 1$. Consideremos três casos separadamente:

(i) $n = 1$: temos $F(1) = \sum_{0<d|1} \mu(d) = \mu(1) = 1$.

(ii) $n = p^k$, com p primo e $k \geq 1$ inteiro: então

$$F(p^k) = \sum_{0<d|p^k} \mu(d) = \sum_{j=0}^{k} \mu(p^j) = \mu(1) + \mu(p) = 0.$$

(iii) $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, com $p_1 < \cdots < p_k$ primos: como F é multiplicativa, segue de (3.1) e do item (ii) que

$$F(n) = F(p_1^{\alpha_1}) \ldots F(p_k^{\alpha_k}) = 0.$$

■

O teorema 3.8 a seguir evidencia o papel central da função de Möbius na teoria das funções aritméticas multiplicativas. Para sua prova, observe que a função

$$\begin{array}{rccc} f: & D(n) & \longrightarrow & D(n) \\ & d & \longmapsto & n/d \end{array} \quad (3.3)$$

é uma bijeção; realmente, como $f \circ f = \mathrm{Id}_{D(n)}$, segue do exemplo 1.40 do volume 3 que f é uma bijeção.

Nas notações da proposição 3.4, a fórmula (3.4) a seguir, conhecida como a **fórmula de inversão de Möbius**, ensina como recuperar a função f a partir da função F (mesmo quando f não for multiplicativa).

Teorema 3.8 (Möbius)**.** Seja $f : \mathbb{N} \to \mathbb{R}$ uma função aritmética qualquer. Se $F : \mathbb{N} \to \mathbb{R}$ é a função dada por $F(n) = \sum_{0<d|n} f(d)$, então

$$f(n) = \sum_{0<d|n} F\left(\frac{n}{d}\right)\mu(d) = \sum_{0<d|n} F(d)\mu\left(\frac{n}{d}\right). \quad (3.4)$$

Prova. A segunda igualdade em (3.4) segue da bijetividade da função em (3.3). Para a primeira igualdade, note inicialmente que

$$\sum_{0<d|n} F\left(\frac{n}{d}\right)\mu(d) = \sum_{0<d|n}\left(\mu(d)\sum_{0<d'|\frac{n}{d}} f(d')\right) = \sum_{0<d|n}\sum_{0<d'|\frac{n}{d}} \mu(d)f(d').$$

Mas, como $d \mid n$ e $d' \mid \frac{n}{d}$ se, e só se, $d' \mid n$ e $d \mid \frac{n}{d'}$, segue daí que

$$\sum_{0<d|n} F\left(\frac{n}{d}\right)\mu(d) = \sum_{0<d'|n}\sum_{0<d|\frac{n}{d'}} \mu(d)f(d') = \sum_{0<d'|n}\left(f(d')\sum_{0<d|\frac{n}{d'}} \mu(d)\right).$$

Agora, se $\frac{n}{d'} > 1$ (i.e., se $d' < n$) a proposição 3.7 fornece

$$\sum_{0<d|\frac{n}{d'}} \mu(d) = 0.$$

Portanto, o penúltimo somatório acima se reduz à parcela correspondente a $d' = n$, de sorte que

$$\sum_{0<d'|n}\left(f(d')\sum_{0<d|\frac{n}{d'}} \mu(d)\right) = f(n)\sum_{0<d|1} \mu(d) = f(n)\mu(1) = f(n).$$

■

Antes de prosseguir com o desenvolvimento da teoria, mostremos por um exemplo como a fórmula de inversão de Möbius pode ser utilizada como ferramenta de contagem.

Exemplo 3.9. Fixado $n \in \mathbb{N}$, dizemos que uma sequência $(x_1, x_2, \ldots, x_n)$, tal que $x_j \in \{0, 1\}$ para $1 \leq j \leq n$, é *aperiódica* se não existir divisor $0 < d < n$ de n tal que a sequência seja formada pela justaposição de $\frac{n}{d}$ cópias do bloco $(x_1, \ldots, x_d)$. Calcule, em função de n, o número de sequências aperiódicas de n termos.

Prova. Note inicialmente que, pelo princípio fundamental da contagem, há exatamente 2^n sequências $(x_1, x_2, \ldots, x_n)$ tal que $x_j \in \{0, 1\}$ para $1 \leq j \leq n$.

Por outro lado, para uma sequência $(x_1, x_2, \ldots, x_n)$ como no enunciado, definimos seu *período* d como o menor divisor positivo de n tal que a sequência seja formada pela justaposição de n/d cópias do bloco $(x_1, \ldots, x_d)$. Em particular, uma sequência aperiódica $(x_1, x_2, \ldots, x_n)$ tem período n.

Mais geralmente, se a sequência $(x_1, x_2, \ldots, x_n)$ tiver período d, então $(x_1, \ldots, x_d)$ será aperiódica, e reciprocamente. Portanto, se a_k denota o número de sequências aperiódicas de k termos, temos

$$\sum_{0<d|n} a_d = 2^n.$$

Aplicando a fórmula de inversão de Möbius, obtemos então

$$a_n = \sum_{0<d|n} \mu\left(\frac{n}{d}\right) 2^d.$$

■

A teoria desenvolvida até o presente momento nos permite introduzir e estudar as principais propriedades de outra importante função aritmética, conforme ensina a definição a seguir.

Definição 3.10. A **função φ de Euler** é a função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por

$$\varphi(n) = \#\{1 \leq k \leq n;\ \text{mdc}\,(k, n) = 1\}.$$

Em palavras, $\varphi(n)$ conta quantos inteiros de 1 a n são primos com n. No que segue, dentre outras propriedades, vamos mostrar que função φ é multiplicativa e usar esse resultado para calcular $\varphi(n)$ em função da decomposição canônica de n em fatores primos[2]. Comecemos com um resultado que será útil em outras circunstâncias.

Proposição 3.11. Se $\varphi : \mathbb{N} \to \mathbb{N}$ é a função de Euler, então

$$\sum_{0<d|n} \varphi(d) = \sum_{0<d|n} \varphi\left(\frac{n}{d}\right) = n.$$

Prova. A primeira igualdade segue da bijetividade da função f em (3.3). Para a segunda igualdade, seja $D(n) = \{1 = a_1 < a_2 < \cdots < a_t = n\}$; se $1 \leq k \leq n$, temos $\text{mdc}\,(k, n) \in D(n)$, i.e., $\text{mdc}\,(k, n) = a_i$ para algum $1 \leq i \leq t$; portanto, sendo $A_i = \{1 \leq k \leq n;\ \text{mdc}\,(k, n) = a_i\}$, segue que

$$I_n = A_1 \cup \ldots \cup A_t,$$

uma união disjunta e, daí, $n = \sum_{i=1}^{t} |A_i|$. Note, agora, que

$$\begin{aligned} A_i &= \{1 \leq k \leq n;\ \text{mdc}\,(k, n) = a_i\} \\ &= \{1 \leq k/a_i \leq n/a_i;\ k/a_i \in \mathbb{N} \text{ e mdc}\,(k/a_i, n/a_i) = 1\} \\ &= \{1 \leq l \leq n/a_i;\ \text{mdc}\,(l, n/a_i) = 1\}, \end{aligned}$$

de maneira que $|A_i| = \varphi\left(\frac{n}{a_i}\right)$. Portanto,

$$n = \sum_{i=1}^{t} |A_i| = \sum_{i=1}^{t} \varphi\left(\frac{n}{a_i}\right) = \sum_{0<d|n} \varphi\left(\frac{n}{d}\right).$$

■

[2]Para uma outra abordagem, veja o problema 2.1.6 do volume 4.

Para o teorema a seguir, também devido a Euler, precisamos do fato, deixado como exercício para o leitor (veja o problema 1), de que o produto de duas funções aritméticas multiplicativas também é uma função multiplicativa.

Teorema 3.12 (Euler). A função de Euler $\varphi : \mathbb{N} \to \mathbb{N}$ é multiplicativa.

Prova. Fazendo $G(n) = n$, a proposição anterior nos dá $\sum_{0<d|n} \varphi(d) = G(n)$. Portanto, segue da fórmula de inversão de Möbius que

$$\varphi(n) = \sum_{0<d|n} \mu(d) G\left(\frac{n}{d}\right) = \sum_{0<d|n} \mu(d) \cdot \frac{n}{d} = n \sum_{0<d|n} \frac{\mu(d)}{d}. \qquad (3.5)$$

Mas como $f(d) = \frac{\mu(d)}{d}$ é uma função multiplicativa (verifique este fato!), segue da proposição 3.4 que a função $F : \mathbb{N} \to \mathbb{R}$, definida por

$$F(n) = \sum_{0<d|n} \frac{\mu(d)}{d},$$

também é multiplicativa. Logo, $\varphi(n) = nF(n)$ é multiplicativa pelo problema 1. ■

Conforme prometido anteriormente, no corolário a seguir relacionamos $\varphi(n)$ com a decomposição canônica do inteiro $n > 1$ em fatores primos.

Corolário 3.13 (Euler). Se a decomposição canônica do inteiro $n > 1$ em primos é $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, então

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right). \qquad (3.6)$$

Prova. Calculemos inicialmente o valor de $\varphi(p^\alpha)$, com p primo e $\alpha \geq 1$ inteiro:

$$\begin{aligned}
\varphi(p^\alpha) &= \#\{1 \leq k \leq p^\alpha;\ \text{mdc}\,(k, p^\alpha) = 1\} \\
&= \#\{1 \leq k \leq p^\alpha;\ \text{mdc}\,(k, p) = 1\} \\
&= \#\left(\{1, 2, 3, \ldots, p^\alpha\} \setminus \{p, 2p, 3p, \ldots, p^{\alpha-1}p\}\right) \\
&= p^\alpha - p^{\alpha-1} \\
&= p^\alpha\left(1 - \frac{1}{p}\right).
\end{aligned}$$

Agora, como φ é multiplicativa, segue de (3.1) que

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{\alpha_1}) \ldots \varphi(p_k^{\alpha_k}) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \ldots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{\alpha_1} \ldots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right).
\end{aligned}$$

■

A fórmula do corolário anterior nos permite deduzir várias propriedades interessantes (e úteis) da função φ de Euler. Colecionamos, a seguir, um exemplo nesse sentido.

Exemplo 3.14. Dado $x \in \mathbb{N}$, mostre que a equação $\varphi(y) = x$ admite no máximo um número finito de soluções $y \in \mathbb{N}$.

Prova. Primeiramente, se $y = p^\alpha z$, com $\alpha \geq 1$, p primo e $\text{mdc}\,(p, z) = 1$, então o caráter multiplicativo da função φ garante que

$$x = \varphi(y) = \varphi(p^\alpha)\varphi(z) = p^{\alpha-1}(p-1)\varphi(z) \geq 2^{\alpha-1},$$

uma vez que $\varphi(z) \geq 1$ e $p \geq 2$. Portanto, tomando logaritmos na base 2, obtemos

$$\alpha \leq 1 + \log_2 x.$$

Ademais, cálculos análogos aos acima fornecem

$$x = p^{\alpha-1}(p-1)\varphi(z) \geq p - 1,$$

donde $p \leq x + 1$.

Portanto, se $y = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ é a fatoração canônica de y em primos e $\alpha = \max\{\alpha_1, \dots, \alpha_k\}$, segue do que fizemos acima que $\alpha \leq 1 + \log_2 x$ e, daí,

$$y \leq (p_1 \dots p_k)^\alpha \leq \left(\prod_{\substack{p \leq x+1 \\ p \text{ primo}}} p \right)^{1+\log_2 x}.$$

■

Problemas – Capítulo 3

1. * Prove que o produto de duas funções aritméticas multiplicativas também é uma função multiplicativa.

2. Prove que, para todo $n \in \mathbb{N}$, temos $\prod_{0<d|n} d = n^{d(n)/2}$.

3. Prove que, para todo $n \in \mathbb{N}$, temos $\frac{s(n)}{d(n)} \geq \sqrt{n}$.

4. (OCM.) Um professor escolheu um inteiro positivo n e, em seguida, propôs a dois estudantes os problemas a seguir: o primeiro estudante deveria calcular o número de pares ordenados (x, y), com x e y inteiros positivos, satisfazendo a equação

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n};$$

o segundo estudante deveria fazer o mesmo em relação à equação

$$\frac{1}{x} - \frac{1}{y} = \frac{1}{n}.$$

Sabendo que a soma das respostas dos estudantes foi 78, mostre que ao menos um deles cometeu um erro de cálculo.

5. (Hungria - adaptado.) Para $n \in \mathbb{N}$ e $0 \leq r \leq 3$, seja $D_r(n)$ o conjunto dos divisores positivos de n que deixam resto r quando divididos por 4.

   (a) Se mdc $(m, n) = 1$, prove que existe uma bijeção natural

   $$(D_1(m) \times D_1(n)) \cup (D_3(m) \times D_3(n)) \longrightarrow D_1(mn);$$

   faça o mesmo para $(D_1(m) \times D_3(n)) \cup (D_3(m) \times D_1(n))$ e $D_3(mn)$.

   (b) Prove que $|D_1(n)| \geq |D_3(n)|$.

6. Um natural $n > 1$ é **perfeito** se $s(n) = 2n$, onde $s(n)$ é a soma dos divisores positivos de n. Prove que:

   (a) Se $n > 1$ é perfeito, então $\sum_{0<d|n} \frac{1}{d} = 2$.

   (b) Se p é um primo tal que $2^p - 1$ também é primo, então $2^{p-1}(2^p - 1)$ é perfeito.

7. O propósito deste problema é estabelecer a recíproca do problema anterior, provando o seguinte teorema de Euler: se n é um número perfeito par[3], então existe um primo p tal que $2^p - 1$ é primo e $n = 2^{p-1}(2^p - 1)$. Para tanto, seja $n = 2^k q$ um número perfeito par, onde $k, q \in \mathbb{N}$ e q ímpar. Faça os seguintes itens:

   (a) Conclua que $(2^{k+1} - 1)s(q) = 2^{k+1} q$ e, a partir daí, mostre que existe $a \in \mathbb{N}$ tal que $q = (2^{k+1} - 1)a$ e $s(q) = 2^{k+1} a$.

[3] Até hoje não se sabe se existem números perfeitos ímpares.

(b) Se $a = 1$, mostre que $2^{k+1} - 1$ é primo, donde $k + 1 = p$, um primo.

(c) Se $a = 2^{k+1} - 1$, mostre que $s(q) \geq 1 + a + a^2 > (a+1)a = 2^{k+1}a$, uma contradição.

(d) Se $a > 1$ e $a \neq 2^{k+1} - 1$, então q tem pelo menos quatro divisores positivos distintos: 1, $2^{k+1} - 1$, a e $(2^{k+1} - 1)a$. Conclua, a partir daí, que $s(q) > 2^{k+1}a$, chegando a uma nova contradição.

8. Um natural n é *abundante* se $s(n) > 2n$. Se a for abundante, mostre que ab é abundante, qualquer que seja $b \in \mathbb{N}$.

9. Seja $f : \mathbb{N} \to \mathbb{R}$ a função definida por $f(1) = 1$ e, para $n > 1$,
$$f(n) = \frac{(-1)^k}{p_1 p_2 \ldots p_k},$$
onde $p_1, p_2, \ldots, p_k$ são os primos distintos que dividem n. Ache todos os $n \in \mathbb{N}$ tais que $\sum_{0<d|n} f(d) = 0$.

10. Se $f : \mathbb{N} \to \mathbb{R}$ é uma função aritmética multiplicativa, prove que
$$\sum_{0<d|n} \mu(d) f(d) = \prod_{\substack{p \text{ primo} \\ p|n}} (1 - f(p)).$$
Em seguida, use esse resultado para provar os dois itens a seguir:

(a) $\sum_{0<d|n} d\mu(d) = \prod_{\substack{p \text{ primo} \\ p|n}} (1 - p)$.

(b) $\sum_{0<d|n} \mu(d)^2 = 2^k$, onde k é o número de fatores primos distintos de n (observe que $k = 0$ se $n = 1$).

11. Prove o **teorema de Liouville**[4]: para cada $n \in \mathbb{N}$, tem-se
$$\left(\sum_{0<j|n} d(j) \right)^2 = \sum_{0<j|n} d(j)^3.$$

[4]Após Joseph Liouville, matemático francês do século XIX.

12. * Seja $f : \mathbb{N} \to \mathbb{R}$ uma função qualquer e $F : \mathbb{N} \to \mathbb{R}$ a função dada por $F(n) = \sum_{0<d|n} f(d)$. Prove que
$$\sum_{k=1}^{n} F(k) = \sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor f(j).$$

13. Seja $f : \mathbb{N} \to \{-1, 1\}$ a função definida por $f(1) = 1$ e, para $n > 1$ inteiro, $f(n) = (-1)^{\alpha_1 + \cdots + \alpha_k}$, onde $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ é a decomposição canônica de n em fatores primos. Prove que, para todo inteiro $n \geq 1$, tem-se
$$\sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor f(j) = \lfloor \sqrt{n} \rfloor.$$

14. (OBM). Prove que, para todo natural $n > 1$, temos
$$n\left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) < \sum_{k=1}^{n} d(k) \leq n\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right).$$

15. Seja F uma função aritmética multiplicativa e $f : \mathbb{N} \to \mathbb{R}$ a função definida implicitamente por $F(n) = \sum_{0<d|n} f(d)$. Prove que f também é uma função aritmética multiplicativa.

16. O objetivo deste problema é dar outra prova do caráter multiplicativo da função φ. Para tanto, para $m, n > 1$ inteiros primos entre si, arranje os naturais de 1 a mn na tabela
$$\begin{array}{ccccc}
1 & 2 & \ldots & k & \ldots & m \\
m+1 & m+2 & \ldots & m+k & \ldots & 2m \\
2m+1 & 2m+2 & \ldots & 2m+k & \ldots & 3m \\
 & & \ldots & & \ldots & \\
(n-1)m+1 & (n-1)m+2 & \ldots & (n-1)m+k & \ldots & mn
\end{array}$$
e faça os seguintes itens:

(a) Um inteiro da tabela é primo com mn se só se for primo com m e com n.

(b) Em uma coluna qualquer, ou todos os elementos são primos com m ou nenhum é primo com m.

(c) Há exatamente $\varphi(m)$ colunas formadas de inteiros primos com m, cada uma delas contendo exatamente $\varphi(n)$ inteiros primos com n.

(d) Conclua que $\varphi(mn) = \varphi(m)\varphi(n)$.

17. Se $F(n) = \sum_{0<d|n} \frac{\varphi(d)}{d}$, calcule $F(n)$ em termos da decomposição canônica de n.

18. Para cada $m \in \mathbb{N}$, seja A_m o conjunto dos pares ordenados (d, n) tais que d é um divisor positivo de m, $1 \leq n \leq m$ e $\text{mdc}\,(d, n) = 1$. Ache todos os $m \in \mathbb{N}$ tais que $|A_m| = 1993$.

19. * Para $n > 2$ inteiro, prove os itens a seguir:

(a) Se $P_n = \{1 \leq k \leq n;\ \text{mdc}\,(k, n) = 1\}$, então a correspondência $d \mapsto n - d$ é uma bijeção de P_n.

(b) $\varphi(n) = 2l$, onde l é o número de elementos de P_n menores ou iguais a $\frac{n-1}{2}$; em particular, $\varphi(n)$ é par.

20. Dados $m, n \in \mathbb{N}$, com $n > 2$, sejam $1 = a_1 < \cdots < a_k = n - 1$ os inteiros positivos primos com n e menores ou iguais a n, e $S_m(n) = \sum_{i=1}^{k} a_i^m$ a soma de suas $m-$ésimas potências. Prove os seguintes itens:

(a) Se $k = 2l$, então $S_m(n) = \sum_{i=1}^{l}(a_i^m + (n - a_i)^m)$. Conclua, a partir daí, que $S_m(n)$ é par se n o for.

(b) $S_m(n) = \sum_{j=0}^{m}(-1)^j \binom{m}{j} n^{m-j} S_j(n)$.

(c) Se m for ímpar, então

$$2S_m(n) = n \sum_{j=0}^{m-1} (-1)^j \binom{m}{j} n^{m-1-j} S_j(n).$$

Conclua, a partir daí, que, $n \mid S_m(n)$ se m for ímpar.

21. Nas notações do enunciado do problema anterior, prove os seguintes itens:

(a) Todo $1 \leq m \leq n$ pode ser unicamente escrito da forma $m = \frac{n}{d} \cdot a$, com $a, d \in \mathbb{N}$ tais que $d \mid n$ e $\text{mdc}\,(a, d) = 1$.

(b) $\sum_{0<d|n} \frac{S_k(d)}{d^k} = \frac{1^k + 2^k + \cdots + n^k}{n^k}$.

(c) $S_k(n) = n^k \sum_{0<d|n} \mu\left(\frac{n}{d}\right)\left(\frac{1^k + 2^k + \cdots + d^k}{d^k}\right)$.

(d) $S_1(n) = \frac{1}{2} n \varphi(n)$.

(e) $S_2(n) = \frac{1}{3} n^2 \varphi(n) + \frac{1}{6} n \prod_{\substack{p \text{ primo} \\ p|n}} (1 - p)$.

CAPÍTULO 4

Cálculo e Teoria dos Números

Neste capítulo, pressupomos que o leitor tenha conhecimentos rudimentares de Cálculo, mais precisamente familiaridade com sequências e séries convergentes, limites de funções e derivadas, sendo o material do volume 3 desta coleção suficiente para nossos propósitos. Apresentaremos alguns exemplos e resultados básicos sobre a distribuição dos números primos ao longo dos naturais, seguindo essencialmente o clássico [2], bem como um interessante resultado assintótico de Cesàro, sobre pares de naturais primos entre si, seguindo o artigo [6].

4.1 Sobre a distribuição dos primos

Um dos primeiros resultados que aprendemos sobre números primos neste livro foi o teorema de Euclides, o qual garante a existência de infinitos números primos. Estes, contudo, não se distribuem de

maneira uniforme ao longo dos naturais. O teorema a seguir, conhecido como o **teorema do número primo**, torna essa afirmativa mais precisa. Antes de enunciá-lo, fixemos uma notação: para cada real positivo x, denotemos por $\pi(x)$ o número de primos menores ou iguais a x.

Teorema 4.1 (Hadamard[1]). Nas notações acima, temos

$$\lim_{x\to+\infty} \frac{\pi(x)}{x/\log x} = 1,$$

onde $\log : (0,+\infty) \to \mathbb{R}$ denota a função logaritmo natural.

A prova do teorema acima foge largamente ao escopo destas notas mas, para o leitor interessado, recomendamos o clássico [3]. Ressaltamos, contudo, que o teorema de Hadamard garante que as funções $\pi(x)$ e $\frac{x}{\log x}$ são *assintoticamente* (i.e., à medida que $x \to +\infty$) iguais.

Anteriormente ao teorema de Hadamard, P. Chebyshev[2] obteve um resultado bem mais simples (mas, ainda assim, muito interessante), garantindo a existência de constantes positivas c e C tais que

$$c\frac{x}{\log x} \leq \pi(x) \leq C\frac{x}{\log x},$$

para todo $x \geq 2$.

A obtenção da segunda desigualdade acima será o objeto do problema 4; para uma prova da primeira, recomendamos ao leitor o excelente livro de G. Andrews ([2]). Por outro lado, segue prontamente da segunda desigualdade que

$$\frac{\pi(x)}{x} \leq \frac{C}{\log x},$$

para todo real $x \geq 2$; em particular, temos

$$\lim_{x\to+\infty} \frac{\pi(x)}{x} = 0. \tag{4.1}$$

[1] Após Jacques Hadamard, matemático francês do século XIX.

[2] Após Pafnuty Chebyshev, matemático russo do século XIX.

Em palavras, (4.1) significa que a quantidade de números primos menores ou iguais a x é um *infinitésimo* em relação a x, i.e., cresce bem mais lentamente que x, à medida que $x \to +\infty$. No que segue, deduziremos a validade desse resultado diretamente, para o quê precisamos, inicialmente, do seguinte resultado.

Proposição 4.2. Se k é um natural qualquer, então

$$\frac{\pi(x)}{x} < \frac{\varphi(k)}{k} + \frac{2k}{x},$$

onde φ é a função de Euler.

Prova. Seja $x > 0$ real, com $\lfloor x \rfloor = kq + r$, onde $0 \leq r < k$, e note que

$$\begin{aligned}\{1,2,\ldots,\lfloor x \rfloor\} &= \cup_{j=0}^{q-1}\{kj+1,kj+2,\ldots,k(j+1)\}\\ &\quad \cup \{kq+1,kq+2,\ldots,kq+r\}.\end{aligned} \tag{4.2}$$

De 1 a k não há mais do que k números primos, obviamente. Por outro lado, se $j \geq 1$, então, para um número do conjunto $\{kj+1,kj+2,\ldots,k(j+1)\}$ ser primo, tal número deve, necessariamente, ser primo com k. Portanto, não há mais do de $\varphi(k)$ números primos no conjunto $\{kj+1,kj+2,\ldots,k(j+1)\}$. Agora, como $q = \lfloor \frac{x}{k} \rfloor$, (4.2) permite estimar $\pi(x)$ pela desigualdade

$$\pi(x) \leq k + (q-1)\varphi(k) + r < 2k + \left\lfloor \frac{x}{k} \right\rfloor \varphi(k) \leq 2k + \frac{x}{k}\varphi(k).$$

Para obter o resultado do enunciado, basta dividirmos ambos os membros da desigualdade acima por x. ■

Mesmo tendo sido obtida por intermédio de uma contagem bastante simples, a proposição anterior permite mostrar que $\pi(x)$ é, quando $x \to +\infty$, um infinitésimo em relação a x. Lembremos, inicialmente, o seguinte resultado (cf. exemplo 3.20 do volume 3).

Lema 4.3. A série harmônica $\sum_{n\geq 1}\frac{1}{n}$ diverge.

Precisamos de mais um lema técnico.

Lema 4.4. Se $m > 1$ é inteiro e $p_1, p_2, \ldots, p_k$ são os primos menores ou iguais a m, então

$$\sum_{n=1}^{m}\frac{1}{n} < \left[\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\right]^{-1}.$$

Prova. Pela fórmula para a soma dos termos de uma série geométrica convergente (cf. proposição 3.21 do volume 3), temos

$$\left[\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\right]^{-1} = \prod_{i=1}^{k}\left(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\cdots\right).$$

Por outro lado, a escolha de p_1, p_2, $\ldots$, p_k, juntamente com o teorema fundamental da aritmética, garante a validade da inclusão

$$\left\{1, \frac{1}{2}, \ldots, \frac{1}{m}\right\} \subset \left\{\frac{1}{p_1^{j_1}p_2^{j_2}\cdots p_k^{j_k}};\ j_1, j_2, \ldots, j_k \geq 0\right\}.$$

Portanto,

$$\sum_{n=1}^{m}\frac{1}{n} < \sum_{j_1,j_2,\ldots,j_k\geq 0}\frac{1}{p_1^{j_1}p_2^{j_2}\cdots p_k^{j_k}} = \prod_{i=1}^{k}\left(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\cdots\right),$$

e o resultado desejado segue imediatamente. ■

De posse dos resultados acima, podemos provar a seguinte versão fraca do teorema de Hadamard.

Teorema 4.5. $\lim_{x\to+\infty}\frac{\pi(x)}{x} = 0$.

Prova. Temos de provar que, dado $\epsilon > 0$ arbitrariamente, existe $x_0 > 0$ tal que $x > x_0 \Rightarrow \frac{\pi(x)}{x} < \epsilon$. Para tanto, sejam $p_1, p_2, \ldots, p_n$ os n primeiros números primos e $k = p_1p_2\ldots p_n$; a proposição 4.2 e a fórmula para $\varphi(k)$ nos dão

$$\frac{\pi(x)}{x} < \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right) + \frac{2p_1p_2\cdots p_n}{x}. \tag{4.3}$$

Agora, os dois lemas anteriores garantem que

$$\lim_{n\to+\infty}\left[\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_n}\right)\right]^{-1} = +\infty,$$

de sorte que

$$\lim_{n\to+\infty}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_n}\right) = 0.$$

Podemos, pois, escolher um natural n tal que

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_n}\right) < \frac{\epsilon}{2}$$

e, a partir daí, pôr $x_0 = \frac{4p_1p_2\cdots p_n}{\epsilon}$. De posse de tais escolhas, para $x > x_0$ temos, a partir de (4.3), que

$$\frac{\pi(x)}{x} < \frac{\epsilon}{2} + \frac{2p_1p_2\cdots p_n}{x} < \frac{\epsilon}{2} + \frac{2p_1p_2\cdots p_n}{x_0} = \epsilon.$$

■

Heuristicamente, podemos dizer que $\sum_{n\geq 1}\frac{1}{n}$ diverge por ter *muitos naturais* (na verdade, todos eles) dentre seus termos. Por outro lado, a proposição 3.22 do volume 3 garante que

$$\sum_{n\geq 1}\frac{1}{n^2} < +\infty; \tag{4.4}$$

portanto, também de um ponto de vista heurístico, podemos atribuir tal convergência ao fato de que há *poucos naturais* dentre seus termos.

Surge, então, uma pergunta natural no contexto de números primos: a série $\sum_{n\geq 1}\frac{1}{p_n}$, onde p_n é o $n-$ésimo primo, tem *muitos* ou *poucos* naturais, no sentido acima? O teorema 4.5 nos encorajaria a dizer que tal série possui poucos naturais. Mas nossa intuição falha nesse ponto, pois, conforme mostraremos a seguir, a série $\sum_{n\geq 1}\frac{1}{p_n}$ é divergente. Antes, contudo, precisamos de um resultado auxiliar.

Lema 4.6. Para todo $x > 0$ tem-se $e^x > 1 + x$.

Prova. Imediato a partir do exemplo 3.9 do volume 4. ∎

Estamos, agora, em condições de apresentar mais um importante resultado devido ao grande L. Euler.

Teorema 4.7 (Euler). Se p_k denota o $k-$ésimo primo, então a série $\sum_{k\geq 1}\frac{1}{p_k}$ é divergente.

Prova. Se $m \in \mathbb{N}$ e $p_1, p_2, \ldots, p_k$ são os primos menores ou iguais a m, é imediato que

$$\left(\sum_{1\leq j<\sqrt{m}}\frac{1}{j^2}\right)\left(1+\sum_{1\leq i\leq k}\ \sum_{1\leq j_1<\cdots<j_i\leq k}\frac{1}{p_{j_1}p_{j_2}\ldots p_{j_i}}\right)\geq\sum_{j=1}^{m}\frac{1}{j}.$$

Observe, agora, que o segundo fator do primeiro membro da desigualdade acima é simplesmente a soma dos inversos dos naturais livres de quadrados e menores ou iguais a m, a qual será denotada, doravante, por $\sum_{\substack{1\leq j\leq m\\ j\text{ ldq}}}\frac{1}{j}$. Portanto, temos, a partir da desigualdade acima, que

$$\left(\sum_{1\leq j<\sqrt{m}}\frac{1}{j^2}\right)\left(\sum_{\substack{1\leq j\leq m\\ j\text{ ldq}}}\frac{1}{j}\right)\geq\sum_{j=1}^{m}\frac{1}{j}.$$

Como $\sum_{j\geq 1}\frac{1}{j}$ diverge e $\sum_{j\geq 1}\frac{1}{j^2}$ converge, concluímos que a

$$\sum_{\substack{j\geq 1\\ j\text{ ldq}}}\frac{1}{j}$$

diverge. Por fim, suponha que a série dos inversos dos primos convirja para um certo real a. Então, para todo $n \in \mathbb{N}$, temos, a partir do lema anterior, que

$$e^a > \exp\left(\sum_{\substack{p<n\\ p\text{ primo}}}\frac{1}{p}\right)=\prod_{\substack{p<n\\ p\text{ primo}}}\exp\left(\frac{1}{p}\right)>\prod_{\substack{p<n\\ p\text{ primo}}}\left(1+\frac{1}{p}\right)=\sum_{\substack{1\leq j<n\\ j\text{ ldq}}}\frac{1}{j},$$

onde $\exp : \mathbb{R} \to \mathbb{R}$ denota a função exponencial de base e. Mas isto é um absurdo, pois já sabemos que a soma dos inversos dos naturais livres de quadrados diverge. ∎

Problemas – Seção 4.1

1. Prove que existe um real positivo x_0 tal que $\pi(x) > \frac{\log x}{2x}$ para $x > x_0$.

2. Para cada $k \geq 1$, seja a_k o $k-$ésimo natural que não é quadrado perfeito. Decida se a série $\sum_{k\geq 1}\frac{1}{a_k}$ converge.

3. Para cada $k \geq 1$, seja a_k o $k-$ésimo natural composto. Decida se a série $\sum_{k\geq 1}\frac{1}{a_k}$ converge.

4. O objetivo deste problema é mostrar que

$$\pi(x) \leq (30\log 2)\frac{x}{\log x}, \tag{4.5}$$

para todo real $x \geq 8$, onde $\log : (0, +\infty) \to \mathbb{R}$ denota a função logaritmo natural. Para tanto, faça os seguintes itens:

   (a) Para todo $n \in \mathbb{N}$, prove que $\binom{2n}{n}$ é divisível por todos os primos p tais que $n < p \leq 2n$. Ademais, $\binom{2n}{n} < 2^{2n}$.

(b) Prove que, para $n \geq 2$, tem-se $\pi(2n) < \pi(n) + (2\log 2)\frac{n}{\log n}$.

(c) Se $f : (0, +\infty) \to \mathbb{R}$ é a função dada por $f(x) = \frac{x}{\log x}$, mostre que f é crescente em $(e, +\infty)$ e que $f\left(\frac{x+2}{2}\right) < \frac{15}{6} f(x)$, para $x \geq 8$.

(d) Use os itens (b) e (c) para concluir que $\pi(2n) < (32\log 2)\frac{n}{\log n}$, para $n \geq 2$.

(e) Deduza que, para todo número real $x \geq 8$, vale (4.5).

5. O objetivo deste problema é estabelecer a recíproca do resultado do problema 17, página 49. Para tanto, dado $n \in \mathbb{N}$, seja $I(n)$ a soma dos maiores divisores positivos ímpares dos números $1, 2, \ldots, n$ e faça os seguintes itens:

(a) Para $n \in \mathbb{N}$, sejam $\tau(n)$ o maior divisor ímpar de n e $i(n)$ o maior ímpar menor ou igual a n. Prove que

$$\begin{aligned} I(n) &= (\tau(1) + \tau(3) + \cdots + \tau(i(n))) \\ &\quad + (\tau(2) + \tau(4) + \cdots + \tau(2\lfloor n/2 \rfloor)) \\ &= \frac{1}{4}(i(n)+1)^2 + I\lfloor n/2 \rfloor). \end{aligned}$$

(b) Nas notações de (a), mostre que

$$I(n) = \frac{1}{4}\sum_{k=0}^{t}(i(q_k)+1)^2,$$

onde 2^t é a maior potência de 2 menor ou igual a n e, para $0 \leq k \leq t$, q_k é o quociente da divisão de n por 2^k.

(c) Use o fato de que $i(q_k) \leq \frac{n}{2^k}$ para obter a estimativa

$$I(n) \leq \frac{1}{4}\left(\frac{n^2}{3}\left(4 - \frac{1}{4^t}\right) + n\left(4 - \frac{1}{2^{t-1}}\right) + t + 1\right).$$

(d) Use o fato de que $t = \lfloor \log_2 n \rfloor \leq n$ para obte a estimativa

$$I(n) \leq \frac{4n^2 + 15n + 3}{12}.$$

(e) Utilize as desigualdades $\lfloor \log_2 n \rfloor \geq 0$ e $2^{\lfloor \log_2 n \rfloor} \geq 2^{\log_2 n - 1} = \frac{n}{2}$ e

$$\tau(q_k) \geq q_k - 1 = \left\lfloor \frac{n}{2^k} \right\rfloor - 1 \geq \frac{n}{2^k} - 2$$

para mostrar, de maneira análoga, que

$$I(n) \geq \frac{4n^2 - 12n - 1}{12}.$$

(f) Se $T(n) = 1 + 2 + \cdots + n$, conclua que

$$\frac{4n^2 - 12n - 1}{6n^2 + 6n} \leq \frac{I(n)}{T(n)} \leq \frac{4n^2 + 15n + 3}{6n^2 + 6n}$$

e, a partir daí, que, se $r \in \mathbb{Q} \setminus \{\frac{2}{3}\}$, então $\frac{I(n)}{T(n)} = r$ para no máximo um número finito de valores de n.

4.2 O teorema de Chebyshev

O teorema do número primo garante que a diferença $\pi(2x) - \pi(x)$ é assintoticamente igual a

$$\frac{2x}{\log(2x)} - \frac{x}{\log x} = \frac{x}{\log x}\left(\frac{\log x - \log 2}{\log x + \log 2}\right).$$

Mas, como

$$\lim_{x \to +\infty} \frac{\log x - \log 2}{\log x + \log 2} = 1,$$

concluímos que $\pi(2x) - \pi(x)$ é assintoticamente igual a $\frac{x}{\log x}$. Ocorre que

$$\lim_{x \to +\infty} \frac{x}{\log x} = +\infty,$$

de sorte que o argumento acima garante que o número de primos entre x e $2x$ cresce sem limite, à medida que $x \to +\infty$.

Nesta seção, provaremos um resultado bem mais fraco que este, também devido a Chebyshev, o qual garante que sempre há pelo menos um número primo entre n e $2n$, para todo inteiro $n > 1$. Para a demonstração do mesmo, precisamos dos dois resultados auxiliares a seguir.

Lema 4.8. Sejam $n, p \in \mathbb{N}$, sendo p primo, e μ_p o expoente da maior potência de p que divide o coeficiente binomial $\binom{2n}{n}$. Então

$$\mu_p = \sum_{j \geq 1} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right).$$

Ademais, se ν_p é o único inteiro tal que $p^{\nu_p} \leq 2n < p^{\nu_p + 1}$ então $\mu_p \leq \nu_p$.

Prova. Para a primeira parte, veja que, como $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, a maior potência de p que divide $\binom{2n}{n}$ é $\frac{p^{e_p(2n)}}{p^{2e_p(n)}}$, onde (cf. seção 1.3) $e_p(2n)$ e $e_p(n)$ denotam, respectivamente, os expoentes das maiores potências de p que dividem $(2n)!$ e $n!$. Portanto,

$$\mu_p = e_p(2n) - 2e_p(n)$$

e basta usar a proposição 1.48 para obter a fórmula do enunciado.

Para a segunda parte, segue da definição de ν_p que

$$j > \nu_p \Rightarrow p^j > 2n \Rightarrow \left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor = 0.$$

Por outro lado, para $j \geq 1$ temos

$$\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor < \frac{2n}{p^j} - 2\left(\frac{n}{p^j} - 1 \right) = 2,$$

de sorte que $\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \leq 1$, para $j \geq 1$. Portanto, segue dos fatos acima que

$$\mu_p = \sum_{j \geq 1} \left(\left\lfloor \frac{2n}{p^j} \right\rfloor - 2 \left\lfloor \frac{n}{p^j} \right\rfloor \right) \leq \sum_{j=1}^{\nu_p} 1 = \nu_p.$$

■

Lema 4.9. Se $x \geq 2$ é um número real, então

$$\prod_{\substack{p \leq x \\ p \text{ primo}}} p < 4^x.$$

Prova. O lema é claramente válido para $2 \leq x \leq 3$. Por outro lado, se ele for válido para $x = n$, onde $n \geq 3$ é um inteiro ímpar, então ele também será verdadeiro para $n \leq y < n + 2$; de fato, nesse caso $n + 1$ é par, de sorte que

$$\prod_{\substack{p \leq y \\ p \text{ primo}}} p = \prod_{\substack{p \leq n \\ p \text{ primo}}} p < 4^n \leq 4^y.$$

Basta, então, mostrarmos que o lema é verdadeiro para $x = n$, onde $n \geq 3$ é um inteiro ímpar. Para tanto, façamos indução sobre $n \geq 3$ inteiro ímpar, observando que já temos a validade do resultado para $n = 3$. Assuma, como hipótese de indução, que ele também é válido para todos os inteiros ímpares menores que um certo inteiro ímpar $n \geq 5$. Defina $k = \frac{n \pm 1}{2}$, onde escolhemos o sinal de tal modo que k seja ímpar. Então, $k \geq 3$ e $n - k$ é um natural par, tal que

$$n - k = 2k \mp 1 - k \leq k + 1.$$

Daí, se p é um primo tal que $k < p \leq n$, então p é ímpar e $p \mid n!$, $p \nmid k!$ e $p \nmid (n-k)!$ (não pode ser $n - k = k + 1 = p$, uma vez que $n - k$ é par). Concluímos, então, que o produto de todos esses primos divide

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

de modo que

$$\prod_{\substack{k < p \leq n \\ p \text{ primo}}} p \leq \binom{n}{k}. \tag{4.6}$$

Agora, nossas escolhas garantem que k e $n-k$ são distintos. Mas como $\binom{n}{k} = \binom{n}{n-k}$ e tais números binomiais são parcelas da expansão binomial de $2^n = (1+1)^n$, segue que $\binom{n}{k} \leq 2^{n-1}$ e (4.6) fornece

$$\prod_{\substack{k<p\leq n \\ p \text{ primo}}} p \leq 2^{n-1}. \tag{4.7}$$

Portanto, segue da hipótese de indução e de (4.7) que

$$\prod_{\substack{p\leq n \\ p \text{ primo}}} p = \left(\prod_{\substack{p\leq k \\ p \text{ primo}}} p\right)\left(\prod_{\substack{k<p\leq n \\ p \text{ primo}}} p\right) < 4^k \cdot 2^{n-1} = 2^{2k+n-1} \leq 2^{2n} = 4^n.$$

■

Chegamos, por fim, ao resultado prometido, conhecido como o **teorema de Chebyshev**.

Teorema 4.10 (Chebyshev)**.** Para cada inteiro $n > 1$, há ao menos um primo entre n e $2n$.

Prova. Faremos um argumento geral para mostrar o resultado para $n \geq 128$. Para $n < 128$ tome $p = 3$ para $n = 2$, $p = 5$ para $n = 3$ e

$$\begin{aligned} p &= 7 \text{ para } 4 \leq n \leq 6; \\ p &= 13 \text{ para } 7 \leq n \leq 12; \\ p &= 23 \text{ para } 13 \leq n \leq 22; \\ p &= 43 \text{ para } 23 \leq n \leq 42; \\ p &= 83 \text{ para } 43 \leq n \leq 82; \\ p &= 131 \text{ para } 83 \leq n \leq 127. \end{aligned}$$

Suponha, agora, que o resultado seja falso para algum $n \geq 128$. Nas notações do lema 4.8, tal suposição garante que

$$\binom{2n}{n} = \prod_{\substack{p\leq 2n \\ p \text{ primo}}} p^{\mu_p} = \prod_{\substack{p\leq n \\ p \text{ primo}}} p^{\mu_p}.$$

Mas, para qualquer primo p tal que $\frac{2n}{3} < p \leq n$, temos

$$p \geq 3, \quad p^2 > \frac{2}{3}np, \quad 1 \leq \frac{n}{p} < \frac{3}{2}, \quad 2 \leq \frac{2n}{p} < 3$$

e, daí, $\frac{2n}{p^2} < \frac{3}{p} \leq 1$; segue que

$$\mu_p = \sum_{j\geq 1}\left(\left\lfloor \frac{2n}{p^j}\right\rfloor - 2\left\lfloor \frac{n}{p^j}\right\rfloor\right) = \left\lfloor \frac{2n}{p}\right\rfloor - 2\left\lfloor \frac{n}{p}\right\rfloor = 2 - 2 = 0.$$

Por outro lado, para qualquer primo p tal que $\sqrt{2n} < p \leq \frac{2n}{3}$, temos $p^2 > 2n$ e segue, do lema 4.8, que $1 \leq \mu_p \leq \nu_p = 1$. Finalmente, para os primos $p \leq \sqrt{2n}$, temos, novamente pelo lema 4.8, que $p^{\mu_p} \leq p^{\nu_p} \leq 2n$.

As estimativas acima nos dão (no que segue, p denota um primo)

$$\begin{aligned} \binom{2n}{n} &= \left(\prod_{p\leq\sqrt{2n}} p^{\mu_p}\right)\left(\prod_{\sqrt{2n}<p\leq\frac{2n}{3}} p^{\mu_p}\right)\left(\prod_{\frac{2n}{3}<p\leq n} p^{\mu_p}\right) \\ &= \left(\prod_{p\leq\sqrt{2n}} 2n\right)\left(\prod_{\sqrt{2n}<p\leq\frac{2n}{3}} p\right) \qquad (4.8) \\ &< 4^{\frac{2n}{3}}\left(\prod_{p\leq\sqrt{2n}} 2n\right), \end{aligned}$$

onde utilizamos o lema 4.9 na desigualdade acima. Por outro lado, uma vez que 9 e os números pares maiores que 2 não são primos, a condição $n \geq 128$ ($\Leftrightarrow \sqrt{2n} \geq 16$) garante que

$$\pi\left(\sqrt{2n}\right) \leq \frac{\sqrt{2n}-1}{2} - 1.$$

Substituindo essa última estimativa em (4.8), chegamos a

$$\binom{2n}{n} < 4^{\frac{2n}{3}}(2n)^{\pi(\sqrt{2n})} < 4^{\frac{2n}{3}}(2n)^{\sqrt{\frac{n}{2}}-1}. \tag{4.9}$$

Por fim, note que $\binom{2n}{n}$ é a maior dentre as $2n+1$ parcelas do desenvolvimento binomial de $4^n = (1+1)^{2n}$. Como a primeira e a última de tais parcelas são iguais a 1, temos $2n\binom{2n}{n} > 4^n$ ou, ainda, $\binom{2n}{n} > \frac{4^n}{2n}$, estimativa que, combinada com (4.9), fornece

$$\frac{4^n}{2n} < 4^{\frac{2n}{3}}(2n)^{\sqrt{\frac{n}{2}}-1}$$

ou, ainda,

$$2^{\frac{2n}{3}} < (2n)^{\sqrt{\frac{n}{2}}}.$$

Tomando logaritmos naturais e dividindo por $\frac{\sqrt{2n}}{6}$, a desigualdade acima pode ser reescrita como

$$\sqrt{8n}\log 2 - 3\log(2n) < 0. \qquad (4.10)$$

Denotando $f(x) = \sqrt{8x}\log 2 - 3\log(2x)$, vem que $f(128) = 8\log 2 > 0$ e

$$f'(x) = \frac{\sqrt{2x}\log 2 - 3}{x} > 0$$

para $x \geq 128$. Assim, f é crescente para $x \geq 128$ e (4.10) é falsa, o que nos dá uma contradição. ■

Problemas – Seção 4.2

1. Se p_n é o n–ésimo primo, prove que $p_{n+1} < 2p_n$.

2. * Prove que, para todo inteiro $n > 1$, existe um primo p cujo expoente na decomposição canônica de $n!$ em primos é igual 1.

3. (Torneio das Cidades.) Prove que, para todo inteiro $n > 1$, o número $1!2!\cdots n!$ não é um quadrado perfeito.

4. Ache todos os $m, n, x, y \in \mathbb{N}$ tais que $m, n > 1$ e $(m!)^x = (n!)^y$.

Para os dois problemas a seguir, o leitor achará conveniente utilizar a seguinte *versão forte* do teorema de Chebyschev: para todo inteiro $n \geq 6$, há pelo menos dois primos entre n e $2n$.

5. Ache todos os $m, n \in \mathbb{N}$ tais que $(n-1)!n! = m!$.

6. Encontre todos os naturais $n > 1$ tais que todo natural $1 < m < n$ que seja relativamente primo com n seja, em verdade, um número primo.

4.3 O teorema de Cèsaro

Em 1881, E. Cesàro[3] provou que a probabilidade de dois números naturais, escolhidos aleatoriamente, serem relativamente primos, é igual a $\frac{6}{\pi^2}$. Terminamos este capítulo apresentando, nesta seção, uma demonstração elementar deste resultado, devido ao professor Hudson N. Lima (cf. [6]). Comecemos com alguns preliminares sobre o cálculo de probabilidades.

Sejam E um conjunto finito e não vazio, dito o **espaço amostral**, e P uma **distribuição de probabilidades** em E, i.e., uma função $P: E \to [0,1]$ tal que

$$\sum_{x\in E} P(x) = 1.$$

Para cada $x \in E$, denominamos $P(x)$ a **probabilidade** de x e dizemos que os elementos de E são **equiprováveis** se

$$P(x) = \frac{1}{|E|}, \ \forall\, x \in E.$$

[3]Ernesto Cesàro, matemático italiano do século XIX.

Um **evento** em E é um subconjunto não vazio X de E, sendo sua probabilidade definida por

$$P(X) = \sum_{x \in X} P(x).$$

Voltando, agora, a nosso problema, seja[4] $E = I_n \times I_n$ e suponha que os elementos de E são equiprováveis, de sorte que a probabilidade de cada um deles é igual a $\frac{1}{n^2}$. Dado $n \in \mathbb{N}$, se P_n é a probabilidade de um par ordenado $(a,b) \in E$ ter suas entradas a e b primas entre si, queremos mostrar que

$$\lim_{n \to \infty} P_n = \frac{6}{\pi^2}.$$

Para tanto, devemos, primeiramente, encontrar uma expressão adequada para P_n e, para tal fim, começamos observando que $P_n = \frac{|X|}{n^2}$, onde

$$X = \{(a,b) \in I_n \times I_n;\ \text{mdc}\,(a,b) = 1\}$$

é o evento de nosso interesse.

Uma contagem elementar fornece

$$\begin{aligned} |X| &= 2\#\{(a,b) \in I_n \times I_n;\ \text{mdc}\,(a,b) = 1 \text{ e } a \leq b\} \\ &\quad -\#\{(a,a) \in I_n \times I_n;\ \text{mdc}\,(a,a) = 1\} \\ &= 2\sum_{b=1}^{n} \#\{a \in I_n;\ \text{mdc}\,(a,b) = 1 \text{ e } a \leq b\} - 1 \\ &= 2\sum_{b=1}^{n} \varphi(b) - 1, \end{aligned}$$

onde φ é a função de Euler. Portanto,

$$P_n = \frac{2\sum_{b=1}^{n} \varphi(b) - 1}{n^2}. \tag{4.11}$$

Precisamos, agora, do seguinte resultado auxiliar.

[4]Como no volume 4, pomos $I_n = \{1, 2, \ldots, n\}$.

Lema 4.11. Se $f : \mathbb{N} \to \mathbb{R}$ é uma função qualquer, então, para n natural, temos:

(a) $\sum_{k=1}^{n} \sum_{0<d|k} f(d) = \sum_{k=1}^{n} f(k) \left\lfloor \frac{n}{k} \right\rfloor$.

(b) $\sum_{k=1}^{n} k \sum_{0<d|k} f(d) = \frac{1}{2} \sum_{k=1}^{n} kf(k) \left\lfloor \frac{n}{k} \right\rfloor \left(\left\lfloor \frac{n}{k} \right\rfloor + 1 \right)$.

Prova. O item (a) é o conteúdo do problema 12, página 87. Quanto ao item (b), observe inicialmente que o conjunto dos pares ordenados (d,k) de inteiros tais que $1 \leq k \leq n$ e $0 < d \mid k$ coincide com o conjunto dos pares ordenados (d,k) de inteiros tais que $1 \leq d \leq n$ e $k = ld$, para algum $1 \leq l \leq n/d$. Portanto, podemos trocar a ordem dos somatórios envolvidos, obtendo

$$\begin{aligned} \sum_{k=1}^{n} k \sum_{0<d|k} f(d) &= \sum_{d=1}^{n} \sum_{\substack{k=ld \\ 1 \leq l \leq \frac{n}{d}}} kf(d) \\ &= \sum_{d=1}^{n} f(d) \cdot \left(d + 2d + \cdots + \left\lfloor \frac{n}{d} \right\rfloor d \right) \\ &= \frac{1}{2} \sum_{d=1}^{n} df(d) \left\lfloor \frac{n}{d} \right\rfloor \left(\left\lfloor \frac{n}{d} \right\rfloor + 1 \right). \end{aligned}$$

■

Lembre-se, agora, de que, de acordo com (3.5),

$$\varphi(n) = n \sum_{0<d|n} \frac{\mu(d)}{d},$$

onde $\mu : \mathbb{N} \to \mathbb{R}$ é a função de Möbius. Portanto, o item (b) do lema

anterior fornece

$$\begin{aligned}
2\sum_{k=1}^{n}\varphi(k) &= 2\sum_{k=1}^{n}k\sum_{0<d|k}\frac{\mu(d)}{d}\\
&= \sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor\left(\left\lfloor\frac{n}{k}\right\rfloor+1\right) \qquad (4.12)\\
&= \sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor^2+\sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor.
\end{aligned}$$

A segunda parcela da última soma acima pode ser calculada com o auxílio do item (a) do lema anterior, juntamente com o resultado da proposição 3.7. De fato, temos

$$\sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor=\sum_{k=1}^{n}\sum_{0<d|k}\mu(d)=1,$$

uma vez que $\sum_{0<d|k}\mu(d)$ só não vale 0 para $k=1$. Segue, pois, de (4.11) e (4.12) que

$$P_n=\frac{1}{n^2}\sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor^2. \qquad (4.13)$$

De posse da fórmula acima, podemos enunciar e provar a proposição a seguir, a qual garante que $\lim_{n\to\infty}P_n$ existe e o expressa como um outro limite que, conforme veremos, pode ser efetivamente calculado. Para o enunciado da mesma, observe inicialmente que, como $|\mu(k)|\leq 1$ para todo $k\in\mathbb{N}$ e a série $\sum_{k\geq1}\frac{1}{k^2}$ é convergente, as proposições 3.25 e 3.29 do volume 3 garantem que a série

$$\sum_{k\geq1}\frac{\mu(k)}{k^2}$$

também é convergente.

Proposição 4.12. Se P_n é definido como acima, então $\lim_{n\to\infty}P_n$ existe e é tal que

$$\lim_{n\to\infty}P_n=\sum_{k\geq1}\frac{\mu(k)}{k^2}.$$

Prova. Inicialmente, obtemos a partir de (4.13) que

$$\begin{aligned}
\left|P_n-\sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right| &= \left|\sum_{k=1}^{n}\mu(k)\left(\frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2-\frac{1}{k^2}\right)\right|\\
&\leq \sum_{k=1}^{n}\left|\frac{1}{k^2}-\frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2\right|.
\end{aligned} \qquad (4.14)$$

A fim de estimar o último somatório acima, afirmamos que, para n e k naturais, com $1\leq k\leq n$, vale

$$\left|\frac{1}{k^2}-\frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2\right|<\frac{2}{nk}-\frac{1}{n^2}.$$

De fato,

$$\begin{aligned}
\frac{n}{k}-1<\left\lfloor\frac{n}{k}\right\rfloor\leq\frac{n}{k} &\Rightarrow \frac{n^2}{k^2}-\frac{2n}{k}+1<\left\lfloor\frac{n}{k}\right\rfloor^2\leq\frac{n^2}{k^2}\\
&\Rightarrow \frac{1}{k^2}-\frac{2}{kn}+\frac{1}{n^2}<\frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2\leq\frac{1}{k^2}\\
&\Rightarrow 0\leq\frac{1}{k^2}-\frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2<\frac{2}{kn}-\frac{1}{n^2},
\end{aligned}$$

conforme desejado.

Voltando a (4.14), obtemos, a partir da estimativa acima, que

$$\left|P_n-\sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right|<\sum_{k=1}^{n}\left(\frac{2}{nk}-\frac{1}{n^2}\right)=\frac{2}{n}\sum_{k=1}^{n}\frac{1}{k}-\frac{1}{n}.$$

Mas, a partir do exemplo 6.47 do volume 3 e da regra de l'Hôspital (cf. problema 6.2.6 do volume 3), temos que

$$\frac{2}{n}\sum_{k=1}^{n}\frac{1}{k}<\frac{2}{n}\left(1+\int_1^n\frac{1}{t}dt\right)=\frac{2}{n}(\log n+1)\to 0$$

quando $n \to +\infty$, onde $\log : (0, +\infty) \to \mathbb{R}$ denota a função logaritmo natural. Portanto,

$$\lim_{n \to +\infty} \left(\frac{2}{n} \sum_{k=1}^{n} \frac{1}{k} - \frac{1}{n} \right) = 0$$

e nossos cálculos acima garantem que

$$\lim_{n \to +\infty} \left(P_n - \sum_{k=1}^{n} \frac{\mu(k)}{k^2} \right) = 0.$$

Por fim, segue, daí, que

$$\lim_{n \to \infty} P_n = \lim_{n \to \infty} \left(P_n - \sum_{k=1}^{n} \frac{\mu(k)}{k^2} \right) + \sum_{k \geq 1} \frac{\mu(k)}{k^2} = \sum_{k \geq 1} \frac{\mu(k)}{k^2}.$$

■

A proposição anterior reduziu a prova do teorema de Cesàro a mostrarmos que

$$\sum_{k \geq 1} \frac{\mu(k)}{k^2} = \frac{6}{\pi^2},$$

o que faremos com o auxílio dos três resultados seguintes.

A prova do teorema a seguir é devido a A. Yaglom e I. Yaglom (cf. capítulo 8 de [1]) e utiliza alguns fatos elementares sobre números complexos e raízes de polinômios. Para uma discussão autocontida, referimos o leitor aos capítulos 3 e 4 do volume 6 desta coleção. Para uma prova alternativa, utilizando a teoria elementar de séries de Fourier, recomendamos o capítulo 1 de [4] ou o capítulo 2 de [10].

Teorema 4.13.

$$\sum_{k \geq 1} \frac{1}{k^2} = \frac{\pi^2}{6}.$$

Prova. A primeira fórmula de de Moivre (cf. proposição 1.6 do volume 6) nos dá

$$\begin{aligned} \operatorname{sen}(n\theta) &= \operatorname{Im}((\cos\theta + i \operatorname{sen}\theta)^n) \\ &= \operatorname{Im}\left\{ \sum_{j=0}^{n} \binom{n}{j} i^j (\cos\theta)^{n-j} (\operatorname{sen}\theta)^j \right\} \\ &= \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \binom{n}{2k+1} (\cos\theta)^{(n-2k-1)} (\operatorname{sen}\theta)^{(2k+1)} \end{aligned}$$

e, daí,

$$\frac{\operatorname{sen}(n\theta)}{(\operatorname{sen}\theta)^n} = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \binom{n}{2k+1} (\operatorname{ctg}\theta)^{(n-2k-1)},$$

sempre que $\operatorname{sen}\theta \neq 0$.

Para $n = 2m + 1$, temos

$$\frac{\operatorname{sen}((2m+1)\theta)}{(\operatorname{sen}\theta)^{(2m+1)}} = \sum_{k=0}^{m} (-1)^k \binom{2m+1}{2k+1} (\operatorname{ctg}\theta)^{(2m-2k)}.$$

Assim, definindo

$$f(x) = \sum_{k=0}^{m} (-1)^k \binom{2m+1}{2k+1} x^{m-k},$$

mostramos que

$$f((\operatorname{ctg}\theta)^2) = \frac{\operatorname{sen}((2m+1)\theta)}{(\operatorname{sen}\theta)^{(2m+1)}}.$$

Definindo $\theta_k = (\frac{k}{2m+1})\pi$, para $k = 1, 2, \ldots, m$, é imediato que $(\operatorname{ctg}\theta_1)^2$, $(\operatorname{ctg}\theta_2)^2$, $\ldots$, $(\operatorname{ctg}\theta_m)^2$ são m raízes distintas de f. Mas, como f tem grau m, concluímos que essas são todas as raízes complexas de f, de sorte que as relações de Girard entre raízes e coeficientes de um polinômio (cf. proposição 4.6 do volume 6) fornecem

$$(\operatorname{ctg}\theta_1)^2 + (\operatorname{ctg}\theta_2)^2 + \cdots + (\operatorname{ctg}\theta_m)^2 = \frac{\binom{2m+1}{3}}{\binom{2m+1}{1}} = \frac{m(2m-1)}{3}$$

ou, ainda,

$$\begin{aligned}(\csc\theta_1)^2+\cdots+(\csc\theta_m)^2 &= (1+(\operatorname{ctg}\theta_1)^2)+\cdots+(1+(\operatorname{ctg}\theta_m)^2)\\ &= m+((\operatorname{ctg}\theta_1)^2+\cdots+(\operatorname{ctg}\theta_m)^2)\\ &= m+\frac{m(2m-1)}{3}=\frac{2m(m+1)}{3}.\end{aligned}$$

Por fim, como $\theta_j \in (0, \frac{\pi}{2})$, para $1 \le j \le m$, as desigualdades (6.8) do volume 3 garantem que

$$\operatorname{sen}\theta_j \le \theta_j \le \operatorname{tg}\theta_j,$$

para $1 \le j \le m$ e, daí, que

$$(\operatorname{ctg}\theta_j)^2 \le \frac{1}{\theta_j^2} \le (\csc\theta_j)^2,$$

para $1 \le j \le m$. Portanto,

$$\frac{m(2m-1)}{3}=\sum_{j=1}^{m}(\operatorname{ctg}\theta_j)^2 \le \sum_{j=1}^{m}\frac{1}{\theta_j^2} \le \sum_{j=1}^{m}(\csc\theta_j)^2=\frac{2m(m+1)}{3}$$

ou, o que é o mesmo,

$$\frac{m(2m-1)}{3} \le \sum_{j=1}^{m}\frac{(2m+1)^2}{\pi^2\cdot j^2} \le \frac{2m(m+1)}{3}.$$

Multiplicando as desigualdades acima por $\frac{\pi^2}{(2m+1)^2}$, fazendo $m \to +\infty$ e observando que

$$\lim_{m\to\infty}\frac{m(2m-1)}{3(2m+1)^2}=\lim_{m\to\infty}\frac{2m(m+1)}{3(2m+1)^2}=\frac{1}{6},$$

obtemos o resultado desejado com o auxílio do teorema do confronto.

■

Teorema 4.14. Se p_n é o n-ésimo número primo, então

$$\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^2}\right)^{-1}=\sum_{k\ge 1}\frac{1}{k^2}.$$

Prova. Como $p_n > n$ para todo $n \in \mathbb{N}$, temos

$$\sum_{k=1}^{n}\frac{1}{k^2} \le \left(1+\frac{1}{p_1^2}+\cdots+\frac{1}{p_1^{2l}}\right)\cdots\left(1+\frac{1}{p_n^2}+\cdots+\frac{1}{p_n^{2l}}\right)$$

para cada $l \ge 1$. Além disso,

$$\left(1+\frac{1}{p_1^2}+\cdots+\frac{1}{p_1^{2l}}\right)\cdots\left(1+\frac{1}{p_n^2}+\cdots+\frac{1}{p_n^{2l}}\right) \le \sum_{k=1}^{p_1^l\cdots p_n^l}\frac{1}{k^2}$$

para cada $l \ge 1$, posto que cada parcela obtida a partir do desenvolvimento do primeiro membro aparece no segundo membro.

Mas, dado que

$$\sum_{k=1}^{p_1^l\cdots p_n^l}\frac{1}{k^2} \le \sum_{k\ge 1}\frac{1}{k^2},$$

temos

$$\sum_{k=1}^{n}\frac{1}{k^2} \le \left(1+\frac{1}{p_1^2}+\cdots+\frac{1}{p_1^{2l}}\right)\cdots\left(1+\frac{1}{p_n^2}+\cdots+\frac{1}{p_n^{2l}}\right) \le \sum_{k\ge 1}\frac{1}{k^2}.$$

Fazendo $l \to +\infty$ e observando (cf. proposição 3.21 do volume 3) que

$$\lim_{l\to\infty}\left(1+\frac{1}{p_i^2}+\cdots+\frac{1}{p_i^{2l}}\right)=\left(1-\frac{1}{p_i^2}\right)^{-1},$$

obtemos

$$\sum_{k=1}^{n}\frac{1}{k^2} \le \left(1-\frac{1}{p_1^2}\right)^{-1}\cdots\left(1-\frac{1}{p_n^2}\right)^{-1} \le \sum_{k\ge 1}\frac{1}{k^2}$$

ou, ainda,

$$\sum_{k=1}^{n} \frac{1}{k^2} \le \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right)^{-1} \le \sum_{k\ge 1} \frac{1}{k^2}.$$

O resultado segue, novamente, do teorema do confronto. ■

Teorema 4.15. Se p_n é o n−ésimo número primo, então

$$\lim_{n\to\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right) = \sum_{k\ge 1} \frac{\mu(k)}{k^2}.$$

Prova. Em tudo o que segue, convencionamos que $l < m \Rightarrow i_l < i_m$. Para $n \in \mathbb{N}$, sejam: A_n o conjunto dos números da forma $p_{i_1}p_{i_2}\cdots p_{i_{2s}}$, onde $s \in \mathbb{N}$, $p_{i_1}, p_{i_2}, \ldots, p_{i_{2s}}$ são primos e $p_{i_1}p_{i_2}\cdots p_{i_{2s}} \le n$; $\tilde{A}_n$ o conjunto dos números da forma $p_{i_1}p_{i_2}\cdots p_{i_{2s}}$, onde $s \in \mathbb{N}$, p_{i_1}, p_{i_2}, $\ldots$, $p_{i_{2s}}$ são primos e $i_1, i_2, \ldots, i_{2s} \le n$; B_n o conjunto dos números da forma $p_{i_1}p_{i_2}\cdots p_{i_{2s+1}}$, onde $s \in \mathbb{N}$, $p_{i_1}, p_{i_2}, \ldots, p_{i_{2s+1}}$ são primos e $p_{i_1}p_{i_2}\cdots p_{i_{2s+1}} \le n$; $\tilde{B}_n$ o conjunto dos números da forma $p_{i_1}p_{i_2}\cdots p_{i_{2s+1}}$, onde $s \in \mathbb{N}$, $p_{i_1}, p_{i_2}, \ldots, p_{i_{2s+1}}$ são primos e $i_1, i_2, \ldots, i_{2s+1}$ n; Sejam, ainda,

$$a_n = 1 + \sum_{x\in A_n} \frac{1}{x^2}, \quad \tilde{a}_n = 1 + \sum_{x\in \tilde{A}_n} \frac{1}{x^2}, \quad b_n = \sum_{x\in B_n} \frac{1}{x^2} \quad \text{e} \quad \tilde{b}_n = \sum_{x\in \tilde{B}_n} \frac{1}{x^2}.$$

É imediato verificar que

$$a_n - b_n = \sum_{k=1}^{n} \frac{\mu(k)}{k^2} \quad \text{e} \quad \tilde{a}_n - \tilde{b}_n = \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right).$$

Além disso, os limites $\lim a_n$, $\lim b_n$, $\lim \tilde{a}_n$ e $\lim \tilde{b}_n$ todos existem, pois as sequências correspondentes são não decrescentes e limitadas superiormente por $\sum_{k=1}^{\infty} \frac{1}{k^2}$. Em particular, esse argumento garante a existência do limite

$$\lim_{n\to\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right).$$

Como $p_n > n$ para todo $n \in \mathbb{N}$, temos $A_n \subseteq \tilde{A}_n \subseteq A_{p_1p_2\ldots p_n}$ e $B_n \subseteq \tilde{B}_n \subseteq B_{p_1p_2\ldots p_n}$; logo, valem as desigualdades

$$a_n \le \tilde{a}_n \le a_{p_1p_2\ldots p_n} \quad \text{e} \quad b_n \le \tilde{b}_n \le b_{p_1p_2\ldots p_n}.$$

Portanto, uma vez mais a partir do teorema do confronto, obtemos

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} \tilde{a}_n \quad \text{e} \quad \lim_{n\to\infty} b_n = \lim_{n\to\infty} \tilde{b}_n,$$

de sorte que

$$\begin{aligned} \lim_{n\to\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right) &= \lim_{n\to\infty} \tilde{a}_n - \lim_{n\to\infty} \tilde{b}_n = \lim_{n\to\infty} a_n - \lim_{n\to\infty} b_n \\ &= \lim_{n\to\infty} \sum_{k=1}^{n} \frac{\mu(k)}{k^2} = \sum_{k\ge 1} \frac{\mu(k)}{k^2}, \end{aligned}$$

conforme desejado. ■

Podemos, finalmente, juntar os resultados acima para calcular

$$\begin{aligned} \lim_{n\to\infty} P_n &= \sum_{k\ge 1} \frac{\mu(k)}{k^2} = \lim_{n\to\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right) \\ &= \left[\lim_{n\to\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right)^{-1}\right]^{-1} \\ &= \left[\sum_{k\ge 1} \frac{1}{k^2}\right]^{-1} = \frac{6}{\pi^2}. \end{aligned}$$

CAPÍTULO 5

A Relação de Congruência

Introduzimos ao leitor, neste capítulo, a importante relação, em $\mathbb{Z}$, de conguência módulo $n > 1$. Nosso objetivo central é provar um famoso teorema de P. de Fermat, conhecido na literatura como o *pequeno teorema de Fermat*, bem como sua generalização igualmente famosa, devido a Euler e conhecida como o *teorema de Euler*. A pervasividade desses resultados em teoria elementar dos números se deve, dentre outros, ao fato dos mesmos iniciarem um estudo sistemático do comportamento dos restos da divisão das potências de um natural a por um natural $n > 1$ fixado, no caso em que a e n são relativamente primos. De fato, de certa forma, tal estudo será nosso objeto principal de investigação a partir de agora, sendo retomado explicitamente no capítulo 7. Apresentamos, também, o não menos famoso *teorema chinês dos restos*, o qual possui muitas aplicações interessantes em teoria elementar dos números.

5.1 Definições e propriedades básicas

O objeto central de estudo nesta seção é a relação entre números inteiros explicitada na definição a seguir.

Definição 5.1. Sejam a, b e n inteiros dados, sendo $n > 1$. Dizemos que a é **congruente** a b, módulo n, e denotamos $a \equiv b \pmod{n}$, se $n \mid (a - b)$. Se a não for congruente a b módulo n, denotamos $a \not\equiv b \pmod{n}$.

Exemplos 5.2. De acordo com a definição acima, podemos escrever:

(a) $3 \equiv 5 \pmod{2}$, pois $2 \mid (3 - 5)$.

(b) $-1 \equiv 11 \pmod{12}$, pois $12 \mid (-1 - 11)$.

(c) $2 \equiv -1 \pmod{3}$, pois $3 \mid (2 - (-1))$.

(d) $x \equiv -x \pmod{2}$, pois $2 \mid (x - (-x))$.

(e) $1 \not\equiv 2 \pmod{3}$, pois $3 \nmid (1 - 2)$.

(f) $20 \not\equiv 15 \pmod{7}$, pois $7 \nmid (20 - 15)$.

O que estamos realmente investigando em um número quando consideramos congruências módulo n? Para responder essa pergunta, observemos o que ocorre com os números inteiros módulo 4, por exemplo:

$$4k \equiv 0 \pmod{4}, \quad 4k + 1 \equiv 1 \pmod{4},$$

$$4k + 2 \equiv 2 \pmod{4} \ \text{ e } \ 4k + 3 \equiv 3 \pmod{4}.$$

Assim, a sequência $\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$ dos números inteiros é igual, módulo 4, à sequência

$$\ldots, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, \ldots$$

e vemos que todo inteiro é congruente, módulo 4, ao resto de sua divisão por 4. Esse resultado continua válido em geral, como mostrado no seguinte resultado.

Proposição 5.3. Sejam a e n inteiros dados, com $n > 1$.

(a) Se a deixa resto r na divisão por n, então $a \equiv r \pmod{n}$. Em particular, todo inteiro é congruente, módulo n, a exatamente um dos números $0, 1, 2, \ldots, n-2, n-1$.

(b) $a \equiv b \pmod{n} \Leftrightarrow a$ e b deixam um mesmo resto na divisão por n.

Prova.
(a) Suponha que a deixa resto r quando dividido por n. Pelo algoritmo da divisão, temos $a = qn + r$ para algum inteiro q. Daí, $a - r = qn$, ou seja, $n \mid (a - r)$. Mas isso é o mesmo que escrevermos $a \equiv r \pmod{n}$. O resto é imediato.

(b) Se $a \equiv b \pmod{n}$, então $n \mid (a - b)$ e segue, do corolário 1.9 (com a e b nos lugares de a_1 e a_2 e n no lugar de b), que a e b deixam um mesmo resto na divisão por n. Reciprocamente, se a, b deixam um mesmo resto r na divisão por n, podemos escrever $a = nq_1 + r$ e $b = nq_2 + r$, com $q_1, q_2 \in \mathbb{Z}$. Logo, $a - b = n(q_1 - q_2)$, ou seja, $n \mid (a - b)$. Portanto, $a \equiv b \pmod{n}$. ■

Observação 5.4. Na definição da relação de congruência, a razão pela qual excluímos o módulo $n = 1$ é a seguinte: se usássemos congruências módulo 1, obteríamos $a \equiv b \pmod{1}$ como sinônimo de $1 \mid (a - b)$, o que é sempre verdade. Portanto, dois inteiros quaisquer seriam indistinguíveis módulo 1.

Uma vez que a notação de congruência módulo n enxerga apenas o resto da divisão de um número por n, o leitor pode estar se perguntando quais vantagens teremos em utilizá-la. O primeiro ganho ao se usar congruências é computacional: nas duas proposições a seguir, provamos algumas propriedades elementares de congruências, as quais vão nos permitir, por exemplo, calcular mecanica e rapidamente

o resto da divisão de 17^{2002} por 13, tarefa que não é fácil de cumprir com os métodos de que dispomos até o presente momento.

Proposição 5.5. Dados inteiros a, b, c e n, sendo $n > 1$, temos:

(a) $a \equiv a \pmod{n}$.

(b) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.

(c) $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Prova. Os itens (a) e (b) são imediatos. Quanto a (c), se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $n \mid (a-b)$ e $n \mid (b-c)$, e o item i. da observação 1.6 garante que n divide $a - c = (a-b) + (b-c)$. Mas isso é o mesmo que $a \equiv c \pmod{n}$. ■

Proposição 5.6. Sejam a, b, c, d, m e n inteiros dados, com $m, n > 1$.

(a) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a + c \equiv b + d \pmod{n}$ e $ac \equiv bd \pmod{n}$. Em particular, $ac \equiv bc \pmod{n}$.

(b) Se $a \equiv b \pmod{n}$, então $a^k \equiv b^k \pmod{n}$, para todo $k \in \mathbb{N}$.

(c) Se $c_0, c_1, \ldots, c_m \in \mathbb{Z}$ e $f(x) = c_m x^m + \cdots + c_1 x + c_0$, então

$$a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n}.$$

(d) Se $a \equiv b \pmod{n}$, então $\text{mdc}\,(a, n) = \text{mdc}\,(b, n)$.

(e) Se $a + c \equiv b + c \pmod{n}$, então $a \equiv b \pmod{n}$.

(f) Se $ac \equiv bc \pmod{n}$ e $\text{mdc}\,(c, n) = d$, então $a \equiv b \pmod{\frac{n}{d}}$. Em particular, se $\text{mdc}\,(c, n) = 1$, então $a \equiv b \pmod{n}$.

(g) Se $a \equiv b \pmod{mn}$, então $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$.

(h) Se $a \equiv b \pmod{n}$ e $a \equiv b \pmod{m}$, com $\text{mdc}\,(m, n) = 1$, então $a \equiv b \pmod{mn}$.

Prova.
(a) Como $(a+c)-(b+d) = (a-b)+(c-d)$, $ac-bd = a(c-d)+(a-b)d$ e $n \mid (a-b)$, $n \mid (c-d)$, segue do item (c) da proposição 1.5 (veja também o item i. da observação 1.6) que $n \mid [(a+c)-(b+d)]$ e $n \mid (ac-bd)$. Mas isso é o mesmo que $a + c \equiv b + d \pmod{n}$ e $ac \equiv bd \pmod{n}$. Por fim, o caso particular segue de $c \equiv c \pmod{n}$.

(b) Fazendo $c = a$ e $d = b$ na segunda parte do item (a), obtemos $a^2 \equiv b^2 \pmod{n}$. Se já mostramos que $a^l \equiv b^l \pmod{n}$, para um certo $l \in \mathbb{N}$, então, novamente da segunda parte de (a) (dessa vez com $c = a^l$ e $d = b^l$), obtemos

$$a^{l+1} = a \cdot a^l \equiv b \cdot b^l = b^{l+1} \pmod{n}.$$

O item (b) segue, por indução sobre k.

(c) Se $a \equiv b \pmod{n}$, temos, a partir dos itens (a) e (b), que $c_k a^k \equiv c_k b^k \pmod{n}$, para $0 \leq k \leq m$. Portanto, segue do problema 1 que

$$f(a) = \sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k = f(b) \pmod{n}.$$

(d) Como $a \equiv b \pmod{n}$, existe $q \in \mathbb{Z}$ tal que $a = b + nq$. Queremos, pois, mostrar que

$$\text{mdc}\,(b + nq, n) = \text{mdc}\,(b, n).$$

Mas isso é imediato a partir do item (b) da proposição 1.21.

(e) Se $a + c \equiv b + c \pmod{n}$, então n divide $(a + c) - (b + c) = a - b$, o que é o mesmo que $a \equiv b \pmod{n}$.

(f) Sejam $n = dn'$ e $c = dc'$, com c' e n' inteiros primos entre si. De $ac \equiv bc \pmod{n}$, segue que $(dn') \mid [dc'(a-b)]$ ou, ainda, que

$n' \mid c'(a-b)$. Mas, como $\text{mdc}\,(n', c') = 1$, segue do item (a) da proposição 1.21 que $n' \mid (a-b)$ ou, o que é o mesmo, $a \equiv b\,(\text{mod}\,\frac{n}{d})$. O resto é imediato.

(g) Se $a \equiv b\,(\text{mod}\,mn)$, então $mn \mid (a-b)$ e, daí, $m \mid (a-b)$. Mas essa última relação equivale a $a \equiv b\,(\text{mod}\,m)$; analogamente, $a \equiv b\,(\text{mod}\,n)$.

(h) Como $m, n \mid (a-b)$ e $\text{mdc}\,(m,n) = 1$, segue do item (d) da proposição 1.21 que $mn \mid (a-b)$, que é o que queríamos provar. ■

Conforme prometido, temos o exemplo seguinte.

Exemplo 5.7. Calcule o resto da divisão do número 17^{2002} por 13.

Solução. Como $17 \equiv 4\,(\text{mod}\,13)$ e $16 \equiv 3\,(\text{mod}\,13)$, segue do item (b) da proposição 5.6 que, módulo 13,

$$17^{2002} \equiv 4^{2002} = 16^{1001} \equiv 3^{1001}.$$

Notando, agora, que $3^3 \equiv 1\,(\text{mod}\,13)$ e aplicando os itens (a) e (b) da proposição 5.6, obtemos

$$3^{1001} = 3^2 \cdot 3^{999} = 9 \cdot (3^3)^{333} \equiv 9 \cdot 1^{333} = 9,$$

módulo 13. Então, segue da proposição 5.3 que 17^{2002} deixa resto 9 na divisão por 13. ■

As propriedades elementares de congruências deduzidas na proposição 5.6 nos permitem provar o critério de divisibilidade por 9 de maneira mais direta que aquela sugerida no problema 1, página 10, conforme o próximo exemplo.

Exemplo 5.8. Para $n \in \mathbb{N}$ mostremos, utilizando congruências, que o resto da divisão de n por 9 é igual ao resto da divisão da soma dos algarismos da representação decimal de n por 9.

Prova. Se $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$ é a representação decimal do natural n, podemos escrever

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0.$$

Como $10 \equiv 1\,(\text{mod}\,9)$, aplicando repetidas vezes as propriedades da proposição 5.6 obtemos, módulo 9, que

$$\begin{aligned} n &= a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_k \cdot 1^k + a_{k-1} \cdot 1^{k-1} + \cdots + a_1 \cdot 1 + a_0 \\ &= a_k + a_{k-1} + \cdots + a_1 + a_0. \end{aligned}$$

O resto segue do item (b) da proposição 5.3. ■

Como exemplo adicional da simplificação computacional que a relação de congruência nos oferece (e para referência futura), provaremos novamente, a seguir, o corolário 1.8 e o exemplo 1.10. Antes, contudo, é útil fazermos uma pequena observação.

Como já sabemos, todo inteiro é congruente a $0, 1, 2, 3, 4, 5$ ou 6, módulo 7; mas como

$$4 \equiv -3(\text{mod}\,7), \quad 5 \equiv -2(\text{mod}\,7) \quad \text{e} \quad 6 \equiv -1(\text{mod}\,7),$$

segue que todo inteiro é congruente, módulo 7, a um dos números $0, \pm 1, \pm 2, \pm 3$. Por outro lado, todo inteiro é congruente a 0, 1, 2, 3, 4, 5, 6 ou 7, módulo 8; mas, como

$$5 \equiv -3(\text{mod}\,8), \quad 6 \equiv -2(\text{mod}\,8) \quad \text{e} \quad 7 \equiv -1(\text{mod}\,8),$$

segue que todo inteiro é congruente a $0, \pm 1, \pm 2, \pm 3$ ou 4, módulo 8. A vantagem de trocar, módulo 7, os números de 0 a 6 por $0, \pm 1, \pm 2, \pm 3$ é que, se precisarmos elevar os restos na divisão por 7 a um expoente par, teremos menos trabalho usando $0, \pm 1, \pm 2, \pm 3$ em vez de

$0, 1, 2, 3, 4, 5, 6$, posto que $(-x)^2 = x^2$. Pela mesma razão, por vezes é vantajoso trocar, módulo 8, os números $0, 1, 2, 3, 4, 5, 6, 7$ por $0, \pm 1, \pm 2, \pm 3, 4$.

Generalizando a discussão do parágrafo anterior, não é difícil verificar que:

i. Se $n = 2k$, então todo inteiro é congruente, módulo n, a um dos números
$$0, \pm 1, \pm 2, \ldots, \pm(k-1), k.$$

ii. Se $n = 2k+1$, então todo inteiro é congruente, módulo n, a um dos números
$$0, \pm 1, \pm 2, \ldots, \pm k.$$

Formalizaremos um pouco mais a discussão acima quando estudarmos *sistemas completos de restos*, na seção 6.1. Por enquanto, vamos ao resultado prometido.

Proposição 5.9. Para todo $a \in \mathbb{Z}$ temos:

(a) $a^2 \equiv 0, 1, 4, 5, 6$ ou $9 \pmod{10}$.

(b) $a^2 \equiv 0$ ou $1 \pmod 3$.

(c) $a^2 \equiv 0$ ou $1 \pmod 4$.

(d) $a^2 \equiv 0, 1$ ou $4 \pmod 8$.

(e) $a^4 \equiv 0$ ou $1 \pmod{16}$.

Prova.
(a) Módulo 10, temos $a \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4$ ou 5, de sorte que
$$a^2 \equiv 0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2, (\pm 4)^2 \text{ ou } 5^2$$

ou, ainda, $a^2 \equiv 0, 1, 4, 9, 6$ ou 5. Mas, como o último algarismo de um número é igual ao resto de sua divisão por 10, segue que o último

algarismo de a^2 é igual a um dos números $0, 1, 4, 5, 6$ ou 9.

(b) Sabemos que $a \equiv 0$ ou $\pm 1 \pmod 3$, de modo que $a^2 \equiv 0^2$ ou $(\pm 1)^2 \pmod 3$. Portanto, $a^2 \equiv 0$ ou $1 \pmod 3$.

(c) Sabemos que $a \equiv 0, \pm 1$ ou $2 \pmod 4$, de maneira que $a^2 \equiv 0^2, (\pm 1)^2$ ou $2^2 \pmod 4$. Como $2^2 \equiv 0 \pmod 4$, segue que $a^2 \equiv 0$ ou $1 \pmod 4$.

(d) Como $a \equiv 0, \pm 1, \pm 2, \pm 3$ ou $4 \pmod 8$, segue que
$$a^2 \equiv 0^2, (\pm 1)^2, (\pm 2)^2, (\pm 3)^2 \text{ ou } 4^2 \pmod 8.$$

Agora, $3^2 = 9 \equiv 1$ e $4^2 = 16 \equiv 0 \pmod 8$, de modo que $a^2 \equiv 0, 1$ ou $4 \pmod 8$.

(e) Pelo item (d), temos que $a^2 = 8q + r$, com $q \in \mathbb{N}$ e $r = 0, 1$ ou 4. Portanto,
$$a^4 = (8q+r)^2 = 16(4q^2 + qr) + r^2 = 16q' + 0 \quad \text{ou} \quad 16q' + 1,$$

com $q' \in \mathbb{N}$. ■

Os exemplos a seguir mostram como podemos usar o que aprendemos até agora sobre congruências para resolver vários problemas interessantes. O leitor deve esforçar-se por assimilar o mais possível as ideias desenvolvidas ao longo das soluções dos mesmos, posto que muitas delas serão de utilidade para a resolução de vários dos problemas propostos nesta seção.

Exemplo 5.10 (Itália). Ache todos os $x, y \in \mathbb{N}$ tais que $x^2 + 615 = 2^y$.

Solução. Analisando a equação dada módulo 3, obtemos
$$x^2 + 0 \equiv (-1)^y \pmod 3.$$

Mas, pelo item (b) da proposição 5.9, temos $x^2 \equiv 0$ ou $1 \pmod 3$, de sorte que a congruência acima nos dá as seguintes possibilidades:

$$0 \equiv (-1)^y \pmod 3 \text{ ou } 1 \equiv (-1)^y \pmod 3.$$

A primeira possibilidade claramente nunca ocorre. Quanto à segunda, se y for ímpar obtemos $1 \equiv -1 \pmod 3$, o que também nunca ocorre. Portanto, y deve ser par, digamos $y = 2z$, com $z > 0$ inteiro. A equação do enunciado pode ser, agora, escrita como

$$615 = 2^{2z} - x^2 = (2^z - x)(2^z + x).$$

Por fim, como $2^z + x > 2^z - x$ e $615 = 3 \cdot 5 \cdot 41$, temos somente as possibilidades

$$\begin{cases} 2^z + x &= 615 \\ 2^z - x &= 1 \end{cases}, \quad \begin{cases} 2^z + x &= 205 \\ 2^z - x &= 3 \end{cases},$$

$$\begin{cases} 2^z + x &= 123 \\ 2^z - x &= 5 \end{cases} \text{ ou } \begin{cases} 2^z + x &= 41 \\ 2^z - x &= 15 \end{cases}.$$

Somando membro a membro as duas equações em cada uma das possibilidades acima, obtemos respectivamente $2^{z+1} = 616, 208, 128$ ou 56. Mas, uma vez que 2^{z+1} uma potência de 2, a única possibilidade viável é que seja $2^{z+1} = 128$, de sorte que

$$\begin{cases} 2^z + x &= 123 \\ 2^z - x &= 5 \end{cases}.$$

Então $z = 6$ e $x = 59$, de modo que a única solução é $x = 59$ e $y = 12$. ∎

Exemplo 5.11 (OIM). Ache todos os $m, n \in \mathbb{N}$ tais que $2^m + 1 = 3^n$.

Solução. Se $m = 1$, então é claro que $n = 1$. Se $m \geq 2$, então $2^m \equiv 0 \pmod 4$; portanto, analisando a equação módulo 4, obtemos

$$1 \equiv (-1)^n \pmod 4,$$

de onde segue que n deve ser par, digamos $n = 2u$, com $u \in \mathbb{N}$. Fazendo esta substituição na equação do enunciado, obtemos $2^m + 1 = 3^{2u}$ ou, ainda,

$$2^m = (3^u - 1)(3^u + 1).$$

Para vermos a que fatoração de 2^m corresponde $(3^u - 1)(3^u + 1)$, seja $d = \text{mdc}\,(3^u - 1, 3^u + 1)$. Então

$$d \mid [(3^u + 1) - (3^u - 1)],$$

ou seja, $d \mid 2$; mas, como $3^u - 1$ e $3^u + 1$ são ambos pares, deve ser $d = 2$. Por outro lado, uma vez que o produto de $3^u - 1$ e $3^u + 1$ é uma potência de 2, cada um dos fatores $3^u - 1$ e $3^u + 1$ deve ser uma potência de 2. Ocorre que o mdc de duas potências de 2 só é igual a 2 quando a menor de tais potências for igual a 2, de modo que a única possibilidade é termos

$$\begin{cases} 3^u - 1 = 2 \\ 3^u + 1 = 2^{m-1} \end{cases}.$$

Logo, $u = 1$, $m = 3$ e, daí, $n = 2$. ∎

Exemplo 5.12. *Faça os seguintes itens:*

(a) Prove que existem $x, y, z \in \mathbb{N}$ tais que $13x^4 + 3y^4 - z^4 = 2013$.

(b) Prove que não existem $x, y, z \in \mathbb{N}$ tais que $13x^4 + 3y^4 - z^4 = 2014$.

Prova (Sketch).
(a) Fazendo $z = 2x$, obtemos $y^4 - x^4 = 671$ ou, ainda, $(y^2 - x^2)(y^2 + x^2) = 11 \cdot 61$. Portanto, $y^2 - x^2 = 11$ e $y^2 + x^2 = 61$, de forma que $x = 5$, $y = 6$ e $z = 10$.

(b) Suponha que haja uma solução. Pelo item (e) da Proposição 5.9, temos $a^4 \equiv 0$ ou $1 (\text{mod. } 16)$, para todo $a \in \mathbb{Z}$. Logo, $13x^4 + 3y^4 - z^4 \equiv 0, 2, 12, 13$ ou $15 \,(\text{mod. } 16)$. Mas, como $2014 \equiv 14 \,(\text{mod. } 16)$, chegamos a uma contradição. ∎

Os dois últimos exemplos que apresentamos resolvidos de forma um pouco mais tersa que os anteriores. Como exercício para o leitor, sugerimos esforçar-se por preencher eventuais detalhes omitidos.

Exemplo 5.13 (Romênia). Sejam $m, n, p \in \mathbb{N}$, com p primo ímpar. Se $\frac{7^m+p\cdot 2^n}{7^m-p\cdot 2^n} \in \mathbb{N}$, prove que tal número é primo.

Prova. Seja $a = \frac{7^m+p\cdot 2^n}{7^m-p\cdot 2^n}$. Como

$$a = 1 + \frac{p\cdot 2^{n+1}}{7^m - p\cdot 2^n} = -1 + \frac{2\cdot 7^m}{7^m - p\cdot 2^n},$$

segue que $(7^m - p\cdot 2^n) \mid \text{mdc}\,(p\cdot 2^{n+1}, 2\cdot 7^m)$. Há, agora, duas possibilidades:

(i) $p = 7$: neste caso,

$$(7^m - 7\cdot 2^n) \mid \text{mdc}\,(7\cdot 2^{n+1}, 2\cdot 7^m) = 14$$

e, daí, $(7^{m-1} - 2^n) \mid 2$. Isso implica que $7^{m-1} - 2^n = 1$; porém, analisando essa equação módulo 3, obtemos $1^{m-1} - (-1)^n \equiv 1 \pmod 3$, o que é um absurdo.

(ii) $p \neq 7$: neste caso, temos $\text{mdc}\,(p\cdot 2^{n+1}, 2\cdot 7^m) = 2$ e, daí, $(7^m - p\cdot 2^n) \mid 2$. Novamente, isso implica $7^m - p\cdot 2^n = 1$ e, analisando tal equação também módulo 3, obtemos $1^m - p\cdot 2^n \equiv 1 \pmod 3$, de sorte que $p = 3$. Segue, então, que $7^m - 3\cdot 2^n = 1$ e $a = 7^m + 3\cdot 2^n$.

Se $m = 1$, então $n = 1$ e, daí, $a = 13$, um número primo. Se $m > 1$, temos $n > 1$ e

$$2^{n-1} = \frac{7^m - 1}{6} = 7^{m-1} + \cdots + 7 + 1.$$

Como a soma dos m números ímpares do segundo membro da igualdade acima deve ser par, segue que m é par, digamos $m = 2k$. Daí, obtemos $49^k - 1 = 3\cdot 2^n$, a partir de onde consideramos dois subcasos:

- Se $k = 1$, então $m = 2$, $n = 4$ e $a = 97$, novamente um número primo.
- Se $k > 1$, então

$$(49 - 1)(49^{k-1} + \cdots + 49 + 1) = 49^k - 1 = 3\cdot 2^n$$

ou, ainda, $49^{k-1} + \cdots + 49 + 1 = 2^{n-3}$. Essa igualdade nos dá, como acima, que k é par. Por fim, sendo $k = 2l$, segue que

$$3\cdot 2^n = 49^{2l} - 1 \equiv (-1)^{2l} - 1 \equiv 0 \pmod 5,$$

um absurdo.

■

Exemplo 5.14 (BMO). Seja $(a_n)_{n\geq 1}$ a sequência definida para $n \geq 1$ por $a_n = 2^n + 49$. Ache todos os $n \geq 1$ tais que $a_n = pq$ e $a_{n+1} = rs$, com p, q, r, s primos tais que $p < q$, $r < s$ e $q - p = s - r$.

Solução. Seja n um natural tal que os termos a_n e a_{n+1} satisfaçam as condições do enunciado. Se $p, r > 3$, então as condições do enunciado garantem que $p, q, r, s \equiv 1$ ou $5 \pmod 6$. Mas, como $5^2 \equiv 1 \pmod 6$, em qualquer caso temos $pq, rs \equiv 1$ ou $5 \pmod 6$. Por outro lado, se k for o número ímpar dentre n e $n+1$, temos $2^k \equiv 2 \pmod 6$, de sorte que $2^k + 49 \equiv 2 + 1 = 3 \pmod 6$, o que é um absurdo. Assim, devemos ter $p \leq 3$ ou $r \leq 3$ e, daí, ao menos um dentre p e r deve ser igual a 3 (já que a_n e a_{n+1} são ímpares).

Se $p \geq r$, então $q = s + p - r \geq s$, de modo que $a_n = pq \geq rs = a_{n+1}$, uma contradição. Assim, $p < r$, de sorte que $p = 3$ e $q = 3 + s - r$. Logo, $a_n = pq = 3(3 + s - r)$. Por outro lado, também temos

$$2a_n = 2^{n+1} + 98 = (2^{n+1} + 49) + 49 = a_{n+1} + 49 = rs + 49$$

e, portanto, $6(3 + s - r) = rs + 49$. Segue que

$$r = 6 - \frac{67}{s+6}$$

e, daí, $s+6=67$. Assim, $s=61$, $r=5$, $q=59$. Então,

$$3\cdot 59 = a_n = 2^n + 49 \Rightarrow 2^n = 128 \Rightarrow n = 7.$$

■

Problemas – Seção 5.1

1. * Generalize o item (a) da proposição 5.6, mostrando que se $m, n > 1$ são naturais e $a_1, \dots, a_m$, $b_1, \dots, b_m$ são inteiros tais que $a_k \equiv b_k \pmod{n}$ para $1 \le k \le m$, então

$$\sum_{k=1}^{m} a_k \equiv \sum_{k=1}^{m} b_k \pmod{n} \quad \text{e} \quad \prod_{k=1}^{m} a_k \equiv \prod_{k=1}^{m} b_k \pmod{n}.$$

2. Encontre o resto da divisão de $1000^{55} + 55^{1000}$ por 7.
3. Mostre que o número $8^{100} + 3^{2001}$ não é um quadrado perfeito.
4. Encontre o resto da divisão do número $7^{3^{10}}$ por 5.
5. Seja $n \in \mathbb{N}$ tal que $n \equiv -1 \pmod{4}$. Prove que existe um primo p tal que $p \mid n$ e $p \equiv -1 \pmod{4}$.
6. * Use o fato de que $2^4 + 5^4 = 641 = 2^7 \cdot 5 + 1$ para provar que $2^{2^5} + 1$ não é um número primo.
7. (IMO.) Encontre o menor inteiro positivo n satisfazendo as duas condições a seguir:

   (a) O último algarismo da representação decimal de n é 6;

   (b) Se apagarmos o algarismo 6 do final de n e o escrevermos imediatamente à esquerda do primeiro algarismo de n, obtemos o número $4n$.

8. Encontre todos os inteiros positivos n tais que $7 \mid (2^n + 3^n)$.
9. Seja $n = (a_k a_{k-1} \dots a_1 a_0)_{10}$ a representação decimal de n. Prove que o resto da divisão de n por 11 é igual ao resto da divisão por 11 do número

$$a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^{k-1} a_{k-1} + (-1)^k a_k.$$

10. A sequência de Fibonacci $(F_k)_{k\ge1}$ é definida por $F_1 = F_2 = 1$ e, para $n \ge 1$, $F_{n+2} = F_{n+1} + F_n$. Qual o resto da divisão de F_{2002} por 5?
11. Ache todos os números primos p e q tais que $p^2 + 3pq + q^2$ seja um quadrado perfeito.
12. (Estados Unidos.) Prove que a equação

$$x_1^4 + x_2^4 + x_3^4 + \cdots + x_{14}^4 = 15999$$

não possui soluções inteiras.

13. (Romênia.) Ache todos os naturais m, n, k tais que $2^m + 3^n = k^2$.
14. (União Soviética.) Ache todas as soluções em inteiros $m, n, p > 1$ da equação

$$1! + 2! + \cdots + n! = m^p.$$

15. (Bulgária.) Ache todos os inteiros positivos x, y e z tais que $3^x + 4^y = 5^z$.
16. (Tchecoslováquia.) Ache todos os inteiros positivos x, y e p tais que p é primo e $p^x - y^3 = 1$.
17. Ache todos os $a, b, c \in \mathbb{N}$ tais que a e b são pares e $a^b + b^a = 2^c$.
18. (Hungria.) Sejam a e b naturais dados e n um inteiro não negativo tal que $a^n \mid b$. Prove que a^{n+1} divide $(a+1)^b - 1$.

19. (OBM.) Ache todas as soluções inteiras positivas da equação $x^2 + 15^a = 2^b$.

20. (França.) Qual o algarismo das unidades da parte inteira de $\frac{10^{1992}}{10^{83}+7}$? Justifique sua resposta.

21. (China - adaptado.) O objetivo deste problema é mostrar que, se $x, y \in \mathbb{N}$ são tais que $7^x - 3^y = 4$, então $x = y = 1$. Para tanto, faça os seguintes itens:

    (a) Use módulo 8 para concluir que não há soluções se x for par.

    (b) Se x for ímpar e $y > 1$, analise a equação módulo 9 para concluir que $x \equiv 2 \pmod 3$ e, portanto, que $x \equiv 5 \pmod 6$.

    (c) Escrevendo $x = 6q + 5$, com $q \in \mathbb{N}$, conclua que $7^x \equiv \pm 2 \pmod{13}$.

    (d) Mostre que toda potência de 3 é congruente a 1, 3 ou 9, módulo 13.

    (e) Supondo que $y > 1$, use os itens (c) e (d) para chegar a uma contradição.

22. (Bulgária - adaptado.) O propósito deste problema é mostrar que, em inteiros não negativos x, y e z, a equação $5^x 7^y + 4 = 3^z$ só tem a solução $x = 1$, $y = 0$ e $z = 2$. Para tanto, faça os seguintes itens:

    (a) Se $x = 0$, a equação se reduz a $7^y + 4 = 3^z$, de maneira que $z \geq 2$. Use módulo 9 para mostrar que, neste caso, não há soluções.

    (b) Para este e os demais itens, suponha $x \geq 1$. Use modulo 5 para conclur que $z = 2t$, para algum $t \in \mathbb{N}$.

    (c) Mostre que $\text{mdc}\,(3^t - 2, 3^t + 2) = 1$; conclua, a partir daí, que: (i) $3^t - 2 = 1$ e $3^t + 2 = 5^x 7^y$, (ii) $3^t - 2 = 5^x$ e $3^t + 2 = 7^y$ ou (iii) $3^t - 2 = 7^y$ e $3^t + 2 = 5^x$.

    (d) No caso (ii), use módulo 3 para concluir que não há soluções.

    (e) No caso (iii), temos $5^x - 7^y = 4$. A partir daí, use módulo 4 para concluir que y é par. Por fim, se $x \geq 2$, use módulo 25 para chegar a uma contradição.

23. (Miklós-Schweitzer.) Para resolver, em inteiros $x, y, z > 1$, a equação $(x + 1)^y - x^z = 1$, faça os seguintes itens:

    (a) Analise a equação módulo $x+1$ para concluir que z é ímpar.

    (b) Escreva $(x + 1)^y = x^z + 1$ e fatore o segundo membro para concluir que x é par; em seguida, escreva $x^{z-1} = \frac{(x+1)^y - 1}{x}$ e fatore o segundo membro para concluir que y também é par.

    (c) Se $x = 2s$ e $y = 2t$, com $s, t \in \mathbb{N}$, mostre que $(x + 1)^t - 1$ e $(x + 1)^t + 1$ têm mdc igual a 2. A partir daí, use módulo x para concluir que $(x + 1)^t - 1 = 2s^z$ e $(x + 1)^t + 1 = 2^{z-1}$.

    (d) Conclua, a partir de $2s^z < 2^{z-1}$, que $s = 1$. Daí, obtenha sucessivamente $x = 2$, $t = 1$, $y = 2$ e $z = 3$.

5.2 Os teoremas de Euler e Fermat

O uso efetivo de congruências para calcular restos é consideravelmente simplificado se encontrarmos expoentes que tornem uma certa potência congruente a 1. Por exemplo, sabendo que $7^3 \equiv 1 \pmod 9$ fica muito mais fácil calcular o resto da divisão de 25^{1001} por 9: como $25 \equiv 7 \pmod 9$, temos

$$25^{1001} \equiv 7^{1001} = (7^3)^{333} \cdot 7^2 \equiv 1^{333} \cdot 49 \equiv 4 \pmod 9.$$

Nessa direção, o propósito desda seção é, fixados inteiros a e n primos entre si, com $n > 1$, encontrar um expoente $k \in \mathbb{N}$ para o qual

$$a^k \equiv 1 \pmod{n}.$$

Para tanto, analisaremos inicialmente o caso em que n é primo, provando um dos mais importantes resultados da teoria elementar de congruências, conhecido na literatura como o **pequeno teorema de Fermat**.

Teorema 5.15 (Fermat). Para $a, p \in \mathbb{Z}$, com p primo, temos $a^p \equiv a \pmod{p}$. Em particular, se $\text{mdc}\,(a,p) = 1$, então

$$a^{p-1} \equiv 1 \pmod{p}. \tag{5.1}$$

Prova. Se $a^p \equiv a \pmod{p}$, então p divide $a^p - a = a(a^{p-1} - 1)$; portanto, se $\text{mdc}\,(a,p) = 1$, (5.1) segue do item (a) da proposição 1.21. Basta, pois, mostrarmos que $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z}$.

Se $p = 2$ o resultado é óbvio, uma vez que $a^2 - a = a(a-1)$, sendo o produto de dois inteiros consecutivos, é par. Suponhamos, então, que $p > 2$ e provemos o resultado, primeiramente para $a > 0$, por indução sobre a. Para $a = 1$ nada há a fazer. Suponha, por hipótese de indução, o teorema válido para um certo valor natural de a, i.e., suponha que $k^p \equiv k \pmod{p}$, para algum $k \in \mathbb{N}$. Para $a = k + 1$, temos

$$(k+1)^p - (k+1) = (k^p - k) + \sum_{j=1}^{p-1} \binom{p}{j} k^{p-j}.$$

Mas, como $p \mid (k^p - k)$ (pela hipótese de indução) e $p \mid \binom{p}{j}$ para $1 \leq j \leq p-1$ (pelo exemplo 1.41), segue que p divide $(k+1)^p - (k+1)$, ou seja, que $(k+1)^p \equiv (k+1) \pmod{p}$.

Analisemos, agora, o caso $a \leq 0$: se $a = 0$, nada há a fazer; se $a < 0$, então, uma vez que p é ímpar, segue do que fizemos acima que

$$a^p = -(-a)^p \equiv -(-a) = a \pmod{p}.$$

■

A seguir, colecionamos algumas aplicações interessantes do pequeno teorema de Fermat.

Exemplo 5.16. Se p e q são primos distintos, prove que pq divide $p^{q-1} + q^{p-1} - 1$.

Prova. Como p e q são primos distintos, temos $\text{mdc}\,(p,q) = 1$. Portanto, pelo pequeno teorema de Fermat, q divide $p^{q-1} - 1$. Mas, como q também divide q^{p-1}, segue que q divide $q^{q-1} + (p^{q-1} - 1)$. Analogamente, p divide $p^{q-1} + (q^{p-1} - 1)$. Por fim, como ambos p e q dividem $p^{q-1} + q^{p-1} - 1$ e $\text{mdc}\,(p,q) = 1$, o item (d) da proposição 1.21 garante que pq divide $p^{q-1} + q^{p-1} - 1$. ■

Exemplo 5.17 (Romênia). Sejam p e q números primos, com $q \neq 5$. Se $q \mid (2^p + 3^p)$, prove que $q > p$.

Prova. Como $q \mid (2^p + 3^p)$, temos claramente $q \neq 2, 3$, de modo que $q > 5$. Portanto, podemos supor que $p > 3$. Se $q \leq p$, então $q - 1 < p$, de sorte que $q - 1$ e p são primos entre si. Nesse caso, o teorema de Bézout garante a existência de $x, y \in \mathbb{N}$ tais que $px = (q-1)y + 1$. Portanto, a partir de $2^p \equiv -3^p \pmod{q}$, obtemos $(2^p)^x \equiv (-3^p)^x \pmod{q}$; mas, como $-3^p = (-3)^p$, segue que

$$2^{(q-1)y+1} \equiv (-3)^{(q-1)y+1} \pmod{q}.$$

Por fim, uma vez que $q \neq 2, 3$, o pequeno teorema de Fermat nos dá $2^{q-1}, (-3)^{q-1} \equiv 1 \pmod{q}$; a partir daí, a congruência acima se reduz a $2 \equiv -3 \pmod{q}$, de maneira que $q = 5$. Por fim, tal conclusão é, claramente, uma contradição. ■

Exemplo 5.18 (BMO). Sejam $p > 2$ um número primo tal que $3 \mid (p-2)$ e

$$S = \{y^2 - x^3 - 1;\ 0 \leq x, y < p \text{ e } x, y \in \mathbb{Z}\}.$$

Prove que S contém não mais que $p - 1$ múltiplos de p.

Prova. Se $0 \leq u, v \leq p-1$ e $u^3 \equiv v^3 \pmod{p}$, afirmamos que $u = v$. De fato, note primeiro que $u^3 \equiv v^3 \equiv 0 \pmod{p}$ se, e só se, $u = v = 0$; por outro lado, para $1 \leq u, v \leq p-1$, segue do pequeno teorema de Fermat e de $p - 1 = 3k + 1$ que

$$u^{3k+1} \equiv v^{3k+1} \pmod{p}. \tag{5.2}$$

Agora,

$$u^3 \equiv v^3 \pmod{p} \Rightarrow u^{3k} \equiv v^{3k} \pmod{p},$$

e segue de (5.2) que

$$u^{3k}u \equiv v^{3k}v \equiv u^{3k}v \pmod{p}.$$

Por fim, cancelando u^3 na congruência acima, obtemos $u \equiv v \pmod{p}$; a condição $1 \leq u, v \leq p-1$ implica, então, $u = v$.

A discussão acima garante que

$$\{x^3;\ 0 \leq x \leq p-1\} = \{0, 1, \ldots, p-1\}; \tag{5.3}$$

por outro lado, $y^2 - x^3 - 1 \in S$ é múltiplo de p se, e só se, $y^2 \equiv x^3 - 1 \pmod{p}$. Portanto, segue de (5.3) que, para cada $0 \leq y \leq p-1$, existe um único $0 \leq x \leq p-1$ para o qual p divide $y^2 - x^3 - 1$.

Isso nos daria no máximo p múltiplos de p em S. Porém, note que $0 = 1^2 - 0^3 - 1 = 3^3 - 2^3 - 1$ é representado duas vezes em S, de sorte que S contém não mais do que $p - 1$ múltiplos de p. ■

Generalizamos o pequeno teorema de Fermat com o seguinte resultado de L. Euler, o qual evidencia a importância da função φ. Para o enunciado do mesmo, observe que, se $a^k \equiv 1 \pmod{n}$, então o item (d) da proposição 5.6 garante que $\text{mdc}\,(a^k, n) = \text{mdc}\,(1, n) = 1$; em particular, $\text{mdc}\,(a, n) = 1$.

Teorema 5.19 (Euler). Se a e n são inteiros primos entre si, com $n > 1$, então

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{5.4}$$

Prova. Sejam p um fator primo de n e k um natural. Provemos inicialmente, por indução sobre k, que

$$a^{\varphi(p^k)} \equiv 1 \pmod{p^k}. \tag{5.5}$$

O caso $k = 1$ se resume ao pequeno teorema de Fermat. Por hipótese de indução, suponha que $a^{\varphi(p^l)} \equiv 1 \pmod{p^l}$, para algum l natural. Então $a^{\varphi(p^l)} = p^l q + 1$ para algum inteiro q e temos

$$\begin{aligned}
a^{\varphi(p^{l+1})} - 1 &= a^{p\cdot\varphi(p^l)} - 1 = (a^{\varphi(p^l)})^p - 1 \\
&= (p^l q + 1)^p - 1 = \sum_{j=0}^{p} \binom{p}{j} (p^l q)^j - 1 \\
&= \binom{p}{1} p^l q + \sum_{j=2}^{p} \binom{p}{j} p^{jl} q^j \\
&= p^{l+1} q + p^{2l} \sum_{j=2}^{p} \binom{p}{j} p^{(j-2)l} q^j. \\
&\equiv 0 \pmod{p^{l+1}},
\end{aligned}$$

uma vez que $2l \geq l + 1$ para todo $l \geq 1$.

Para terminar, seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ a decomposição canônica de n em fatores primos, de maneira que (cf. teorema 3.12)

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}).$$

Fazendo $m_j = \varphi(p_1^{\alpha_1}) \ldots \widehat{\varphi(p_j^{\alpha_j})} \ldots \varphi(p_k^{\alpha_k})$ (onde o $\widehat{\ }$ sobre um fator significa que o mesmo é omitido do produto correspondente), temos $\varphi(n) = \varphi(p_j^{\alpha_j}) m_j$ e segue de (5.5) que

$$a^{\varphi(n)} = \left(a^{\varphi(p_j^{\alpha_j})}\right)^{m_j} \equiv 1^{m_j} \equiv 1 \pmod{p_j^{\alpha_j}};$$

mas, como os $p_j^{\alpha_j}$ são dois a dois primos entre si, o item (h) da proposição 5.6 garante que $a^{\varphi(n)} \equiv 1 \pmod{n}$. ■

Colecionamos, nos exemplos a seguir, algumas aplicações interessantes do teorema de Euler.

Exemplo 5.20 (OBM). Prove que existe um inteiro $k > 2$ tal que o número $1\underbrace{99\ldots9}_{k}1$ é um múltiplo de 1991.

Prova. Observe primeiramente que

$$1\underbrace{99\ldots9}_{k}1 = 2 \cdot 10^{k+1} - 9.$$

Portanto, queremos achar $k > 2$ inteiro tal que

$$2 \cdot 10^{k+1} - 9 \equiv 0 \pmod{1991}$$

ou, ainda, $2 \cdot 10^{k+1} \equiv 9 \pmod{1991}$. Mas, como $2 \cdot 10^3 \equiv 9 \pmod{1991}$, temos

$$\begin{aligned} 2 \cdot 10^{k+1} \equiv 9 \pmod{1991} &\Leftrightarrow 2 \cdot 10^{k+1} \equiv 2 \cdot 10^3 \pmod{1991} \\ &\Leftrightarrow 10^{k-2} \equiv 1 \pmod{1991}. \end{aligned}$$

Para o que falta, veja que $1991 = 11 \cdot 181$ e 181 é primo (pelo crivo de Eratóstenes, por exemplo). Portanto, $\varphi(1991) = \varphi(11) \cdot \varphi(181) = 10 \cdot 180 = 1800$ e segue, do teorema de Euler, que $10^{1800} \equiv 1 \pmod{1991}$. Logo, basta tomarmos $k - 2 = 1800$. ■

Exemplo 5.21 (Romênia). Sejam a e n naturais dados. Mostre que, do conjunto

$$\{a^2 + a - 1, a^3 + a^2 - 1, a^4 + a^3 - 1, \ldots\},$$

podemos escolher n elementos dois a dois primos entre si.

Prova. Por indução, seja $k \in \mathbb{N}$ e suponha que já provamos a existência de um conjunto $B_k \subset A$ tal que $|B_k| = k$ e os elementos de B_k sejam dois a dois primos entre si. Seja

$$m = \prod_{x \in B_k} x.$$

Como $m \equiv 1 \pmod{a}$, temos $\operatorname{mdc}(a, m) = 1$. Daí, o teorema de Euler nos dá $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Se $y = a^{\varphi(m)+1} + a^{\varphi(m)} - 1$, então $y \in A$; afirmamos que $\operatorname{mdc}(y, x) = 1$, para todo $x \in B_k$. Para tanto, basta mostrarmos que $\operatorname{mdc}(y, m) = 1$. Mas, novamente pelo teorema de Euler,

$$y = a^{\varphi(m)+1} + a^{\varphi(m)} - 1 \equiv a + 1 - 1 = a \pmod{m},$$

e o item (d) da proposição 5.6 garante que

$$\operatorname{mdc}(y, m) = \operatorname{mdc}(a, m) = 1.$$

Portanto, o conjunto $B_{k+1} = B_k \cup \{y\}$ é formado por $k+1$ elementos de A, dois a dois primos entre si, o que completa o passo de indução. ■

Para o próximo exemplo observe que, se $a, k \in \mathbb{N}$, então a representação decimal de a^k tem exatamente $\lfloor k \log_{10} a \rfloor + 1$ algarismos. De fato, sendo m o número de algarismos de a^k, temos $10^{m-1} \le a^k < 10^m$ e, daí,

$$m - 1 \le \log_{10} a^k < m;$$

portanto, $m - 1 = \lfloor \log_{10} a^k \rfloor = \lfloor k \log_{10} a \rfloor$, conforme desejado.

Exemplo 5.22. Prove que existe uma potência de 2 com 1000 zeros consecutivos em sua representação decimal.

Prova. Queremos encontrar $m \in \mathbb{N}$ tal que a representação decimal de 2^m seja da forma

$$2^m = (** \ldots * \underbrace{00\ldots0}_{1000} ** \ldots *)_{10}.$$

Alternativamente, denotando por A e B os naturais formados pelos algarismos de 2^m situados respectivamente à direita e à esquerda da

sequência de 1000 zeros consecutivos, queremos encontrar $m \in \mathbb{N}$ tal que

$$2^m = B \cdot 10^{1000+a} + A,$$

onde a representação decimal de A tem, no máximo, a algarismos.

Para tanto, se fizermos $k = 1000 + a$ e $A = 2^k$, teremos $2^m = B \cdot 10^{1000+a} + A$ se, e só se, a representação decimal de 2^k tiver no máximo $k - 1000$ algarismos e $2^{m-k} = B \cdot 5^k + 1$; esta última condição, por sua vez, se dará se, e só se, $2^{m-k} \equiv 1 \pmod{5^k}$.

Temos, pois, de mostrar que é possível obter $k, m \in \mathbb{N}$ tais que: (i) $m > k$; (ii) a representação decimal de 2^k tem no máximo $k - 1000$ algarismos; (iii) $2^{m-k} \equiv 1 \pmod{5^k}$. Comecemos analisando as condições (i) e (iii).

Pelo teorema de Euler, temos $2^{\varphi(5^k)} \equiv 1 \pmod{5^k}$. Mas, como $\varphi(5^k) = 4 \cdot 5^{k-1}$, deve existir um inteiro positivo q tal que $2^{4 \cdot 5^{k-1}} = 5^k q + 1$. Fazendo, agora, $m = k + 4 \cdot 5^{k-1}$, temos $m > k$ e $2^{m-k} \equiv 1 \pmod{5^k}$.

Resta, agora, mostrarmos ser possível encontrar $k \in \mathbb{N}$ tal que a representação decimal de 2^k tenha no máximo $k - 1000$ algarismos. Para tanto, a discussão que precede este exemplo garante que a representação decimal de 2^k tem exatamente $\lfloor k \log_{10} 2 \rfloor + 1$, de sorte que é suficiente pedir que valha a desigualdade

$$\lfloor k \log_{10} 2 \rfloor + 1 \leq k - 1000.$$

Mas, como

$$k - \lfloor k \log_{10} 2 \rfloor > k - k \log_{10} 2 = k \log_{10} 5,$$

basta tomar, para começar, um natural k tal que $k \log_{10} 5 > 1001$ (o que é certamente possível). ■

Problemas – Seção 5.2

1. (Eslovênia.) São dados vários inteiros cuja soma é igual a 1496. É possível que a soma de suas sétimas potências seja 1999?

2. (Austrália.) Se p é um número primo, prove que o número

$$\underbrace{11\ldots11}_{p}\underbrace{22\ldots22}_{p}\ldots\underbrace{99\ldots9}_{p}-123456789$$

é divisível por p.

3. Dada uma sequência $(x_1, x_2, x_3, \ldots, x_{2n-2}, x_{2n-1}, x_{2n})$ de números reais, uma operação permitida é trocá-la pela sequência

$$(x_{n+1}, x_1, x_{n+2}, x_2, \ldots, x_{2n-1}, x_{n-1}, x_{2n}, x_n).$$

Suponha que começamos com a sequência $(1, 2, 3, \ldots, 2n-2, 2n-1, 2n)$, onde $2n + 1$ é um número primo. Mostre que, após $2n$ repetições da operação acima, todos os números voltarão às suas posições originais.

4. (BMO.) Prove que a equação $y^2 = x^5 - 4$ não possui soluções inteiras.

5. (Estados Unidos.) Dado um primo p, prove que há infinitos naturais n tais que p divide $2^n - n$.

6. (Romênia.) Prove que não existe um inteiro $n > 1$ tal que n divida $3^n - 2^n$.

7. (Bulgária - adaptado.) Dados números primos p e q, faça os seguintes itens:

   (a) Se $p \mid (5^p - 2^p)$, então $p = 3$.

   (b) Se $p \geq q$ e $q \mid (5^p - 2^p)$, então $q = 3$.

(c) Ache todos os p e q tais que $pq \mid (5^p - 2^p)(5^q - 2^q)$.

8. (BMO.) Prove que, para todo natural n dado, existe um natural $m > n$ tal que a representação decimal de 5^m é obtida da representação decimal de 5^n pelo acréscimo de algarismos à esquerda de 5^n.

9. (IMO.) Prove que, para cada inteiro $n > 1$, existem inteiros k_1, $k_2, \ldots, k_n > 1$, dois a dois distintos e tais que os números $2^{k_1} - 3$, $2^{k_2} - 3, \ldots, 2^{k_n} - 3$ são dois a dois primos entre si.

10. Se $(a_n)_{n \geq 1}$ é a sequência de inteiros positivos definida implicitamente por
$$\sum_{0<d|n} a_d = 2^n,$$
prove que $n \mid a_n$ para todo $n \in \mathbb{N}$.

11. (Irã - adaptado.) O teorema de Euler garante que, para $n > 2$ inteiro, todo fator primo de n também é fator primo de $2^{\varphi(n)} - 1$. A afirmação recíproca, entretanto, não é verdadeira, i.e., se $n > 3$ é ímpar, então $2^{\varphi(n)} - 1$ sempre tem fatores primos que não são fatores primos de n. Para provar esse fato faça os seguintes itens:

   (a) Sejam $p_1, \ldots, p_k$ primos ímpares e dois a dois distintos, tais que $k > 1$ ou $p_1 \neq 3$. Mostre que não existem inteiros $\alpha_1, \ldots, \alpha_k \geq 0$, não todos nulos, tais que
$$2^{(p_1-1)\ldots(p_k-1)} - 1 = p_1^{\alpha_1} \ldots p_k^{\alpha_k}.$$

   (b) Conclua que, se $n \neq 1, 3^k$ é um inteiro positivo ímpar, então existe um primo p tal que $p \nmid n$ mas $p \mid (2^{\varphi(n)} - 1)$.

   (c) Se $n = 3^k$, $k \geq 2$, mostre que $2^{\varphi(n)} - 1 \equiv 0 \pmod{7}$.

12. O propósito deste problema é provar o seguinte resultado, conhecido como o **teorema de Sophie Germain**[1]: se p é um primo tal que $2p + 1 = q$ também é primo e, se x, y, z são inteiros tais que $x^p + y^p + z^p = 0$, então p divide ao menos um dentre x, y, z. Para tanto, mostre as afirmações a seguir:

   (a) Podemos supor que x, y e z são dois a dois relativamente primos e que $p > 2$.

   (b) Se $x^p + y^p + z^p = 0$, então $p \mid (x + y + z)$.

   (c) Por contradição suponha, doravante, que $p \nmid x, y, z$. Se $r \neq p$ é um divisor primo de $y + z$, então
$$y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1} \equiv py^{p-1} \pmod{r}.$$

   (d) Conclua, a partir de (c), que $r \nmid (y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1})$ e, daí, que $\text{mdc}\,(y + z, y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1}) = 1$.

   (e) Mostre que existem $a, b, c, d \in \mathbb{Z}$ tais que $y + z = a^p$, $z + x = b^p$, $x + y = c^p$ e $y^{p-1} - y^{p-2}z + \cdots - yz^{p-2} + z^{p-1} = d^p$.

   (f) Como $p = \frac{q-1}{2}$, temos $x^{\frac{q-1}{2}} + y^{\frac{q-1}{2}} + z^{\frac{q-1}{2}} = 0$. Use o pequeno teorema de Fermat para concluir que $q \mid xyz$.

   (g) Se $q \mid x$, deduza que $b^p + c^p - a^p \equiv 0 \pmod{q}$. Substitua $p = \frac{q-1}{2}$ e use novamente o pequeno teorema de Fermat para mostrar que $q \mid abc$.

      i. Se $q \mid b$ ou $q \mid c$, conclua que $q \mid x, y$ ou $q \mid x, z$, contradizendo o item (a). Logo, $q \mid a = (y + z)$.

      ii. Segue de (c) que $d^p \equiv py^{p-1} \equiv pc^{p(p-1)} \pmod{q}$. Substitua $p = \frac{q-1}{2}$ e use o pequeno teorema de Fermat uma vez mais para concluir que $\pm 1 \equiv p \pmod{q}$, chegando assim a uma nova contradição.

[1]Marie-Sophie Germain, matemática francesa dos séculos XVIII e XIX.

13. (Índia - adaptado.) Para cada $x \in \mathbb{N}$, seja $S(x)$ o conjunto

$$S(x) = \{y \in \mathbb{N};\ \varphi^{(k)}(y) = x, \text{ para algum } k \in \mathbb{N}\},$$

onde φ é a função de Euler, $\varphi^{(1)} = \varphi$ e $\varphi^{(k)}$ é a composta k vezes de φ, para $k > 1$. Seja também

$$T = \{2^a \cdot 3^b;\ a, b \in \mathbb{Z}_+, a \geq 1\}.$$

Os passos abaixo mostram que $x \in T \Leftrightarrow S(x)$ é infinito:

(a) Prove que $x \in T \Rightarrow S(x)$ infinito.

(b) Para cada $x \in \mathbb{N}$, seja $u(x)$ o expoente da maior potência de 2 que divide x. Prove que $u(\varphi(x)) \geq u(x)$.

(c) Se $x \notin T$, prove que $u(\varphi(x)) = u(x)$ se, e só se, $x = 2^m p^a$, onde $m \in \mathbb{N}$ e $p \geq 7$ é um primo tal que $p \equiv 3 \pmod 4$.

(d) Se $x \notin T$ é tal que $u(\varphi^{(2)}(x)) = u(\varphi(x)) = u(x)$, prove que o natural a do item (c) é igual a 1.

(e) Prove que, sendo $S(x)$ infinito, existem $a_1, a_2, a_3, \ldots \in \mathbb{N}$ tais que

$$x = a_1,\ a_1 = \varphi(a_2),\ a_2 = \varphi(a_3),\ a_3 = \varphi(a_4), \ldots$$

(f) Suponha ainda $S(x)$ infinito. Utilizando o item (b) prove que existe $n \in \mathbb{N}$ tal que

$$u(a_n) = u(a_{n+1}) = u(a_{n+2}) = \cdots.$$

(g) Conclua do item (d) que, em relação ao inteiro n do item (f), se $i \geq n+2$, então existem um primo $p_i \geq 7$ tal que $p_i \equiv 3 \pmod 4$ e $m_i \in \mathbb{N}$ tal que $a_i = 2^{m_i} p_i$. Prove, em seguida, que $m_{n+2} = m_{n+3} = \cdots$ e, para todo $i > 1$, $p_i = 2p_{i-1} + 1$.

(h) Prove que não há sequência infinita $q_1, q_2, q_3, \ldots$ de primos com $q_i = 2q_{i-1} + 1$, para todo $i > 1$.

(i) Conclua que $S(x)$ infinito $\Rightarrow x \in T$.

5.3 Congruências lineares e o teorema chinês dos restos

Nesta seção, estudamos equações e sistemas de equações simples envolvendo congruências.

Consideremos inicialmente **congruências lineares**, i.e., congruências da forma

$$ax \equiv b \pmod n, \tag{5.6}$$

onde a, b, n são inteiros dados, com $a \neq 0$, $n > 1$, e procuramos as **soluções** (ou **raízes**) $x \in \mathbb{Z}$, i.e., os inteiros x para os quais (5.6) é verdadeira.

Como caso particular da situação acima, dizemos que a é **invertível**, módulo n, se, para $b = 1$, a congruência linear (5.6) tiver solução, i.e., se existir $x \in \mathbb{Z}$ tal que

$$ax \equiv 1 \pmod n.$$

Um tal inteiro x é denominado um **inverso** de a módulo n e, a esse respeito, temos o seguinte resultado.

Proposição 5.23. Um inteiro a é invertível módulo n se, e só se, $\text{mdc}\,(a, n) = 1$. Neste caso, quaisquer dois inversos de a módulo n são congruentes, módulo n.

Prova. Se a for invertível módulo n, existe $x \in \mathbb{Z}$ tal que $ax \equiv 1 \pmod n$. Daí, existe $y \in \mathbb{Z}$ para o qual $ax = ny + 1$ ou, ainda, $xa + (-y)n = 1$. Sabemos pelo corolário 1.15 que, neste caso, $\text{mdc}\,(a, n) = 1$.

Reciprocamente, recorde que o teorema de Bézout garante que o mdc de dois inteiros sempre pode ser escrito como combinação linear dos mesmos. Portanto, se $\text{mdc}\,(a, n) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + ny = 1$ e segue, daí, que $ax \equiv 1 \pmod n$.

Por fim, sejam x e y inversos de a, módulo n. Então

$$ax \equiv 1 \equiv ay \pmod{n},$$

de sorte que $ax \equiv ay \pmod{n}$. Mas, como $\text{mdc}\,(a,n) = 1$, segue da proposição 5.6 que $x \equiv y \pmod{n}$. Assim a possui, módulo n, um único inverso. ■

Corolário 5.24. Se $a, p \in \mathbb{Z}$, com p primo, então a é invertível módulo p se, e só se, $p \nmid a$. Ademais, nesse caso o inverso de a módulo p é único.

Prova. Imediata a partir do fato de que $\text{mdc}\,(a,p) = 1 \Leftrightarrow p \nmid a$. ■

Corolário 5.25. Sejam $a, b, n \in \mathbb{Z}$, com $n > 1$. Se a for invertível, módulo n, então a congruência $ax \equiv b \pmod{n}$ possui uma única solução, módulo n, qual seja,

$$x \equiv a^{\varphi(n)-1}b \pmod{n}.$$

Em particular, todo inverso de a, módulo n, é congruente a $a^{\varphi(n)-1}$, módulo n.

Prova. Se a for invertível, módulo n, então $\text{mdc}\,(a,n) = 1$. Portanto, aplicando sucessivamente o item (f) da proposição 5.6 e o teorema de Euler, obtemos

$$ax \equiv b \pmod{n} \Leftrightarrow a^{\varphi(n)}x \equiv a^{\varphi(n)-1}b \pmod{n} \Leftrightarrow x \equiv a^{\varphi(n)-1}b \pmod{n}.$$

■

Uma vez que dois inversos de a módulo n são sempre congruentes, módulo n, diremos doravante que a possui um único inverso, módulo n, o qual será denotado por a^{-1} quando não houver perigo de confusão com o inverso usual $\frac{1}{a}$ de a em relação à multiplicação em $\mathbb{Q}$.

Como aplicação da noção de inverso módulo n, provemos um famoso *critério de primalidade* conhecido como o **teorema de Wilson**[2].

[2]Após John Wilson, matemático inglês do século XVII.

Teorema 5.26 (Wilson)**.** Um natural p é primo se e só se

$$(p-1)! \equiv -1 \pmod{p}.$$

Prova. Se $p = mn$, com $1 < n < p$, então $(p-1)! \equiv -1 \pmod{p}$ implica $(p-1)! \equiv -1 \pmod{n}$, uma vez que $n \mid p$. Por outro lado, como $1 < n \leq p-1$, temos que $n \mid (p-1)!$, i.e., $(p-1)! \equiv 0 \pmod{n}$. Portanto, $0 \equiv (p-1)! \equiv -1 \pmod{n}$, de maneira que $n \mid 1$, uma contradição.

Reciprocamente, se p é primo, considere a função

$$f : \{1, 2, \ldots, p-1\} \to \{1, 2, \ldots, p-1\},$$

que associa a cada $a \in \{1, 2, \ldots, p-1\}$ seu inverso $a^{-1} \in \{1, 2, \ldots, p-1\}$, módulo p. O corolário 5.25 garante que f é uma bijeção, com $f(a) = b \Leftrightarrow f(b) = a$. Ademais,

$$\begin{aligned} f(a) = a \quad &\Leftrightarrow \quad a^2 \equiv 1 \pmod{p} \\ &\Leftrightarrow \quad p \mid (a^2 - 1) \\ &\Leftrightarrow \quad p \mid (a-1) \text{ ou } p \mid (a+1) \\ &\Leftrightarrow \quad a = 1 \text{ ou } p-1. \end{aligned}$$

Portanto, existem $a_1, \ldots, a_{\frac{p-3}{2}} \in \{1, 2, \ldots, p-1\}$ tais que

$$\{1, 2, \ldots, p-1\} = \{1, p-1\} \bigcup_{i=1}^{\frac{p-3}{2}} \{a_i, a_i^{-1}\}.$$

Por fim, segue, daí e de $a_i a_i^{-1} \equiv 1 \pmod{p}$ para $1 \leq i \leq \frac{p-3}{2}$, que

$$(p-1)! = (p-1) \prod_{i=1}^{\frac{p-3}{2}} (a_i a_i^{-1}) \equiv -1 \pmod{p}.$$

■

Voltando a equações envolvendo congruências, uma generalização natural da congruência linear (5.6) é obtida considerando soluções de um *sistema de congruências lineares*. Nesse sentido, o teorema a seguir, conhecido como o **teorema chinês dos restos**, examina a existência de soluções para tais sistemas.

Teorema 5.27. Sejam $m_1, m_2, \ldots, m_k$ naturais maiores que 1 e dois a dois primos entre si. Dados inteiros quaisquer $a_1, a_2, \ldots, a_k$, o sistema de congruências lineares

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \ldots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{5.7}$$

admite uma única solução, módulo $m_1 m_2 \ldots m_k$. De outro modo, existe um único $0 \le y < m_1 m_2 \cdots m_k$ tal que $x \in \mathbb{Z}$ satisfaz o sistema acima se, e só se,

$$x \equiv y \pmod{m_1 m_2 \ldots m_k}.$$

Prova. Note primeiramente que, se x_1 e x_2 forem duas soluções quaisquer do sistema acima, então

$$x_1 \equiv a_i \equiv x_2 \pmod{m_i}, \ \forall\, 1 \le i \le k.$$

Mas, como $m_1, \ldots, m_k$ são dois a dois primos entre si, segue da proposição 5.6 que

$$x_1 \equiv x_2 \pmod{m_1 m_2 \ldots m_k}.$$

Portanto, se o sistema (5.7) tiver uma solução, esta será única, módulo $m_1 m_2 \ldots m_k$.

Para a existência de solução defina, para $1 \le j \le k$,

$$y_j = \prod_{\substack{1 \le i \le k \\ i \ne j}} m_i,$$

de sorte que $\text{mdc}\,(y_j, m_j) = 1$. Seja b_j o inverso de y_j módulo m_j e $x = \sum_{j=1}^{k} a_j b_j y_j$. Fixado $1 \le l \le k$, temos que $m_l \mid y_j$ para $j \ne l$ e, daí, módulo m_l temos que

$$x \equiv a_l b_l y_l \equiv a_l \cdot 1 \equiv a_l \pmod{m_l}.$$

■

O problema 5 oferece uma demonstração alternativa para a existência de soluções para o sistema de congruências lineares (5.7). Para terminar esta seção, vejamos um exemplo que mostra como é possível aplicar o teorema chinês dos restos para conseguir resultados interessantes[3].

Exemplo 5.28. Mostre, utilizando o teorema chinês dos restos, que, dado $n > 1$ inteiro, existem n naturais consecutivos, todos compostos.

Prova. Escolha n primos distintos $p_1, p_2, \ldots, p_n$ e considere o sistema de congruências

$$\begin{cases} x \equiv -1 \pmod{p_1^2} \\ x \equiv -2 \pmod{p_2^2} \\ \quad \ldots \\ x \equiv -n \pmod{p_n^2} \end{cases}.$$

Como $p_1, p_2, \ldots, p_n$ são dois a dois primos entre si, o teorema chinês dos restos garante a existência de $m \in \mathbb{N}$ satisfazendo o sistema acima. Portanto, $p_j^2 \mid (m + j)$ para $1 \le j \le n$, de maneira que $m + 1, m + 2, \ldots, m + n$ são naturais consecutivos e compostos. ■

Problemas – Seção 5.3

[3]A esse respeito, veja também os problemas 10, página 200, e 4, página 207.

1. Sejam a, b, n inteiros dados, com $n > 1$. Em relação à congruência linear $ax \equiv b \pmod{n}$, prove que:

   (a) Há solução se, e só se, $\text{mdc}\,(a, n) \mid b$.

   (b) Se $\text{mdc}\,(a, n) \mid b$, então a congruência linear do enunciado possui exatamente $\text{mdc}\,(a, n)$ soluções incongruentes, módulo n.

2. Sejam $a_1, a_2, \ldots, a_k, b, n$ inteiros dados, com $n > 1$. Prove que a congruência

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b \pmod{n}$$

possui solução se, e só se, $\text{mdc}\,(a_1, a_2, \ldots, a_k, n) \mid b$.

3. Um grupamento de soldados foi disposto em um bloco retangular, com várias fileiras. O comandante observou que, ao colocar 12 soldados por fileira, sobraram 7 soldados e, ao colocar 13 soldados por fileira, sobraram 5 soldados. Sabendo que o total de soldados estava situado entre 600 e 700, pergunta-se: quantos soldados havia?

4. Nas hipóteses do teorema 5.27, faça os seguintes itens:

   (a) Mostre que resolver (5.7) para $k = 2$ equivale a resolver, em $u, v \in \mathbb{Z}$, a equação Diofantina linear

$$m_1u - m_2v = a_2 - a_1.$$

   (b) Mostre que resolver (5.7) equivale a encontrar tods os $y \in \mathbb{Z}$ que resolvem o sistema de congruências lineares

$$\begin{cases} m_1y \equiv a_2 - a_1 \pmod{m_2} \\ m_1y \equiv a_3 - a_1 \pmod{m_3} \\ \quad\cdots \\ m_1y \equiv a_k - a_1 \pmod{m_k} \end{cases}.$$

   (c) Utilize o procedimento delineado nos itens (a) e (b) para encontrar todas as soluções do sistema de congruências lineares

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{11} \\ x \equiv 9 \pmod{13} \end{cases}.$$

5. Nas notações do teorema 5.27, se $y_j = \prod_{\substack{1 \le i \le k \\ i \neq j}} m_i$ para $1 \le j \le k$, prove que $x = \sum_{j=1}^{k} a_j y_j^{\varphi(m_j)}$ resolve o sistema de congruências lineares (5.7).

6. Seja $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... a sequência dos números primos. Mostre que existe um número natural que deixa resto $2^{p_{k-1}} - 1$ quando dividido por $2^{p_k} - 1$, para $2 \le k \le 100$.

7. Prove que há sequências arbitrariamente longas de inteiros positivos e consecutivos, nenhum dos quais é uma potência de expoente maior que 1.

8. Sejam $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ a decomposição canônica do inteiro $m > 1$ em fatores primos e f um polinômio de coeficientes inteiros.

   (a) Prove que a congruência $f(x) \equiv 0 \pmod{m}$ tem uma solução inteira se, e só se, cada uma das congruências $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, $1 \le i \le k$, tiver solução[4].

   (b) Para $t \in \mathbb{N}$, denote por $N(t)$ o número de soluções inteiras, duas a duas incongruentes, módulo t, para a congruência $f(x) \equiv 0 \pmod{t}$. Mostre que $N(m) = N(p_1^{\alpha_1}) \ldots N(p_k^{\alpha_k})$.

9. Se, em uma progressão aritmética não constante de números naturais, com termo inicial e razão primos entre si, um dos termos

[4]Se p é primo e α é natural, uma condição suficiente para a existência de soluções para uma congruência da forma $f(x) \equiv 0 \pmod{p^\alpha}$ será apresentada no problema 3.4.8 do volume 6.

for um quadrado perfeito e outro for um cubo perfeito, prove que há um termo que é uma sexta potência[5].

[5]As exigências de que a PA seja não constante e tenha primeiro termo e razão primos entre si são desnecessárias, só tendo sido colocadas a fim de simplificar a solução do problema.

CAPÍTULO 6

Classes de Congruência

Fixado um inteiro $n > 1$, a proposição 5.5 garante que a relação $\sim$, definida em $\mathbb{Z}$ por

$$a \sim b \Leftrightarrow a \equiv b \,(\mathrm{mod}\, n),$$

é uma relação de equivalência em $\mathbb{Z}$, denominada a **relação de congruência módulo n**. Nesta seção, estudamos tal relação sob o ponto de vista mais geral das relações de equivalência, para o quê o leitor pode acha conveniente reler as partes pertinentes da seção 2.3 do volume 4. Alternativamente, sugerimos a referência [8].

6.1 Sistemas de restos

Para $a \in \mathbb{Z}$, definimos a **classe de congruência** de a, módulo n, como a classe de equivalência $\overline{a}$ de a com respeito à relação de

congruência módulo n:

$$\begin{aligned} \overline{a} &= \{x \in \mathbb{Z};\ x \equiv a \pmod{n}\} \\ &= \{x \in \mathbb{Z};\ x = a + nq,\ \exists\, q \in \mathbb{Z}\} \\ &= \{\ldots, -2n+a, -n+a, a, n+a, 2n+a, \ldots\}. \end{aligned}$$

Fixado $a \in \mathbb{Z}$, sabemos que existe um único inteiro $0 \leq r < n$ (o resto da divisão de a por n) tal que $a \equiv r \pmod{n}$. Assim, $\{0, 1, \ldots, n-1\}$ é um SRD para a relação de congruência módulo n e a proposição 2.15 e a relação (2.10) do volume 4 fornecem a partição

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \cdots \cup \overline{n-1}. \tag{6.1}$$

Mais geralmente, temos a definição a seguir.

Definição 6.1. Um **sistema completo de restos** módulo n, (abreviamos SCR) é um SRD para a relação de congruência módulo n.

Dado $n > 1$ inteiro, segue de (6.1) que todo SCR, módulo n, é um conjunto $\{a_0, a_1, \ldots, a_{n-1}\}$ de inteiros tais que $a_r \equiv r \pmod{n}$ para $0 \leq r < n$. Equivalentemente, um conjunto de n inteiros é um SCR, módulo n, se, e só se, seus elementos forem dois a dois incongruentes, módulo n.

Exemplo 6.2. Para $n > 1$ inteiro, o conjunto $\left\{x \in \mathbb{Z};\ -\frac{n}{2} \leq x < \frac{n}{2}\right\}$ é um SCR, módulo n. De fato, observe inicialmente que, se $-\frac{n}{2} \leq x < y < \frac{n}{2}$, então $x \not\equiv y \pmod{n}$, uma vez que $0 < y - x < n$; basta, agora, considerar separadamente os casos n par e n ímpar a fim de mostrar que o conjunto em questão possui exatamente n elementos.

A proposição a seguir ensina como construir novos SCR's a partir de outros já conhecidos.

Proposição 6.3.

(a) Sejam a, b e n inteiros dados, com $n > 1$ e a e n primos entre si. Se o conjunto $\{x_0, x_1, \ldots, x_{n-1}\}$ é um SCR, módulo n, então o conjunto $\{ax_0 + b, ax_1 + b, \ldots, ax_{n-1} + b\}$ também o é.

(b) Sejam m e n inteiros maiores do que 1 e primos entre si. Se os conjuntos $\{x_0, x_1, \ldots, x_{m-1}\}$ e $\{y_0, y_1, \ldots, y_{n-1}\}$ são SCR's módulos m e n, respectivamente, então o conjunto

$$\{nx_i + my_j;\ 0 \leq i < m,\ 0 \leq j < n\}$$

é um SCR módulo mn.

Prova.
(a) Como todo SCR módulo n tem n elementos, basta mostrarmos que, se $0 \leq i, j < n$ e

$$ax_i + b \equiv ax_j + b \pmod{n},$$

então $i = j$. Para tanto, segue da congruência acima que $ax_i \equiv ax_j \pmod{n}$. Agora, como $\mathrm{mdc}\,(a, n) = 1$, o item (f) da proposição 5.6 garante que $x_i \equiv x_j \pmod{n}$. Por fim, como $\{x_0, x_1, \ldots, x_{n-1}\}$ é um SCR, módulo n, esta última congruência nos dá $i = j$.

(b) Analogamente ao item (a), basta mostrarmos que, se $0 \leq i, j < m$, $0 \leq k, l < n$ e

$$nx_i + my_k \equiv nx_j + my_l \pmod{mn},$$

então $i = j$ e $k = l$. Supondo a validade da congruência acima, temos, pelo item (g) da proposição 5.6,

$$nx_i + my_k \equiv nx_j + my_l \pmod{m} \quad \text{e} \quad nx_i + my_k \equiv nx_j + my_l \pmod{n}$$

e, daí,

$$nx_i \equiv nx_j \pmod{m} \quad \text{e} \quad my_k \equiv my_l \pmod{n}.$$

Mas, como m e n são primos entre si, aplicando novamente o item (f) da proposição 5.6, obtemos

$$x_i \equiv x_j \pmod{m} \quad \text{e} \quad y_k \equiv y_l \pmod{n}.$$

Por fim, uma vez que $\{x_0, x_1, \ldots, x_{m-1}\}$ e $\{y_0, y_1, \ldots, y_{n-1}\}$ são SCR's módulos m e n, respectivamente, temos $i = j$ e $k = l$. ■

O exemplo a seguir traz uma bela aplicação combinatória do conceito de sistema completo de restos.

Exemplo 6.4 (IMO). Seja p um primo ímpar. Calcule quantos subconjuntos de p elementos do conjunto $\{1, 2, \ldots, 2p\}$ são tais que a soma de seus elementos é divisível por p.

Solução. Seja $\mathcal{F}$ a família dos $\binom{2p}{p} - 2$ subconjuntos de p elementos do conjunto $\{1, 2, \ldots, 2p\}$, diferentes dos conjuntos $X = \{1, 2, \ldots, p\}$ e $Y = \{p+1, p+2, \ldots, 2p\}$ (observe que esses dois conjuntos têm soma de elementos iguais a múltiplos de p).

Definamos em $\mathcal{F}$ uma relação $\sim$ tal que $A \sim B$ se, e somente se, as seguintes condições forem satisfeitas:

(a) Existe $0 \leq r \leq p-1$ tal que $(A \cap X) + r = B \cap X \pmod{p}$.

(b) $A \cap Y = B \cap Y$.

(Aqui, consoante a discussão que precede o exemplo 2.21 do volume 4, para $r \in \mathbb{R}$ e $Z \subset \mathbb{R}$, definimos $Z + r = \{z + r;\ z \in Z\}$.)

É imediato verificar que $\sim$ é uma relação de equivalência em $\mathcal{F}$; por outro lado, fixado $A \in \mathcal{F}$ e $B \in \overline{A}$ (a classe de equivalência de A em $\mathcal{F}$), temos

$$B = (B \cap X) \cup (B \cap Y) = [(A \cap X) + r] \cup (A \cap Y);$$

portanto, a classe $\overline{A}$ terá tantos conjuntos quantos forem os conjuntos distintos da forma $(A \cap X) + r$, quando r varia de 0 a $p-1$.

Denote $A' = A \cap X$ e $S' = \sum_{x \in A'} x$. Como $A \neq X, Y$, temos $\emptyset \neq A' \neq X$, de maneira que $1 \leq |A'| \leq p-1$. Portanto,

$$\sum_{x \in A'+r} x = \sum_{x \in A'} x + r|A'| = S' + r|A'|.$$

Por outro lado, uma vez que $\text{mdc}\,(|A'|, p) = 1$, a proposição 6.3 garante que, à medida que r varia de 0 a $p-1$, os números $S' + r|A'|$ formam um SCR módulo p; em particular, as somas $\sum_{x \in A'+r} x$ são duas a duas distintas, de maneira que os conjuntos $A', A'+1, \ldots, A'+(p-1)$ também são dois a dois distintos. Logo, a classe $\overline{A}$ tem exatamente p conjuntos, e segue da proposição 2.17 do volume 4 que há exatamente

$$\frac{1}{p}\left(\binom{2p}{2} - 2\right)$$

classes de equivalência distintas.

Se mostrarmos que em cada classe há exatamente um conjunto cuja soma de elementos é um múltiplo de p, seguirá que o número pedido de conjuntos é

$$\frac{1}{p}\left(\binom{2p}{2} - 2\right) + 2$$

(não podemos esquecer dos conjuntos X e Y!).

Para o que falta, fixado $A \in \mathcal{F}$ (e, portanto, a classe $\overline{A}$), seja $A'' = A \cap Y$. Queremos contar quantos são os inteiros $0 \leq r \leq p-1$ tais que a soma dos p elementos do conjunto

$$B = [(A \cap X) + r] \cup (A \cap Y) = (A' + r) \cup A''$$

seja um múltiplo de p (lembre-se de que o conjunto B acima é um elemento genérico da classe $\overline{A}$). Mas, para um tal B, segue do que

fizemos acima que

$$\begin{aligned}\sum_{x\in B} x &= \sum_{x\in A'+r} x + \sum_{x\in A''} x \\ &= \sum_{x\in A'} x + r|A'| + \sum_{x\in A''} x \\ &= \sum_{x\in A} x + r|A'| = S + r|A'|,\end{aligned}$$

onde $S = \sum_{x\in A} x$. Portanto, tal soma será congruente a 0 módulo p se, e só se,

$$|A'|r \equiv -S \pmod{p}.$$

Mas, como $\text{mdc}\,(|A'|, p) = 1$, sabemos do corolário 5.24 que existe um único $0 \leq r \leq p-1$ tal que a congruência acima é satisfeita. ■

Voltando ao desenvolvimento da teoria, dados $q, r \in \mathbb{Z}$, com $0 \leq r < n$, lembre que $\text{mdc}\,(nq + r, n) = \text{mdc}\,(r, n)$. Assim, podemos definir o mdc entre uma classe de congruência módulo n e n pondo

$$\text{mdc}\,(\overline{r}, n) = \text{mdc}\,(x, n), \text{ para qualquer } x \in \overline{r}; \tag{6.2}$$

em particular,

$$\text{mdc}\,(\overline{r}, n) = \text{mdc}\,(r, n).$$

Note que, pela proposição 5.23, as classes de congruência $\overline{r}$ tais que $\text{mdc}\,(\overline{r}, n) = 1$ são exatamente as formadas pelos inteiros invertíveis módulo n. Temos, então, a seguinte definição.

Definição 6.5. Um **sistema completo de invertíveis** módulo n (abreviamos **SCI**) é um conjunto I de inteiros tal que

$$|I \cap \overline{r}| = \begin{cases} 1, & \text{se } \text{mdc}\,(\overline{r}, n) = 1 \\ 0, & \text{se } \text{mdc}\,(\overline{r}, n) \neq 1 \end{cases},$$

para toda classe de congruência $\overline{r}$, módulo n.

Fixado $n > 1$ inteiro, como caso particular mais importante da definição acima temos que o conjunto

$$\{x \in \mathbb{Z};\ \text{mdc}\,(x, n) = 1 \text{ e } 1 \leq x \leq n\}$$

é um SCI módulo n.

Mais geralmente, se I for um SCI módulo n, então (6.2) garante facilmente que $|I| = \varphi(n)$, onde φ é a função de Euler. Por outro lado, é claro que I pode ser aumentado a um SCR módulo n e que todo SCR módulo n contém um SCI módulo n.

A proposição a seguir ensina como construir novos SCI's a partir de outros já conhecidos.

Proposição 6.6. Sejam $m, n > 1$ inteiros dados.

(a) Se a é um inteiro primo com n e $\{x_1, x_2, \ldots, x_{\varphi(n)}\}$ é um SCI módulo n, então $\{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}$ também é um SCI módulo n.

(b) Se $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ e $\{y_1, y_2, \ldots, y_{\varphi(n)}\}$ são SCI módulos m e n, respectivamente, então

$$\{nx_i + my_j;\ 1 \leq i \leq \varphi(m),\ 1 \leq j \leq \varphi(n)\} \tag{6.3}$$

é um SCI módulo mn.

Prova.

(a) Como todo SCI é parte de um SCR, segue do item (a) da proposição 6.3 que

$$ax_i \not\equiv ax_j \pmod{n},\ \forall\ 1 \leq i < j \leq \varphi(n).$$

Basta, pois, mostrarmos que $\text{mdc}\,(ax_i, n) = 1$, o que é imediato.

(b) Utilizando novamente o fato de que todo SCI é parte de um SCR, o item (b) da proposição 6.3 garante que o conjunto em (6.3) tem

exatamente $\varphi(m)\varphi(n)$ elementos. Mas, como $\varphi(m)\varphi(n) = \varphi(mn)$ (recorde-se de que $\text{mdc}\,(m,n) = 1$), concluímos que tal conjunto tem $\varphi(mn)$ elementos. Portanto, para mostrarmos que se trata de um SCI módulo mn, basta provarmos que

$$\text{mdc}\,(nx_i + my_j, mn) = 1$$

para todos $1 \leq i \leq \varphi(m)$, $1 \leq j \leq \varphi(n)$. Para tanto, segue dos itens (b) e (c) da proposição 1.21 que

$$\text{mdc}\,(nx_i + my_j, m) = \text{mdc}\,(nx_i, m) = \text{mdc}\,(x_i, m) = 1$$

e, analogamente, $\text{mdc}\,(nx_i + my_j, n) = 1$; portanto, aplicando mais uma vez o item (c) daquele resultado, obtemos $\text{mdc}\,(nx_i+my_j, mn) = 1$. ■

De posse do conceito de SCI e do item (a) da proposição anterior podemos dar uma outra prova do teorema de Euler.

Teorema 6.7 (Euler)**.** Se a e n são inteiros primos entre si, com $n > 1$, então

$$a^{\varphi(n)} \equiv 1 \,(\text{mod}\, n). \tag{6.4}$$

Prova. Sejam $k = \varphi(n)$ e $\{x_1, x_2, \ldots, x_k\}$ um SCI módulo n. Pela proposição 6.6, o conjunto $\{ax_1, ax_2, \ldots, ax_k\}$ também é um SCI módulo n; portanto, módulo n, os inteiros $ax_1, ax_2, \ldots, ax_k$ são, em alguma ordem, congruentes aos inteiros $x_1, x_2, \ldots, x_k$ e segue, daí, que

$$a^k x_1 x_2 \cdots x_k = ax_1 \cdot ax_2 \cdots ax_k \equiv x_1 x_2 \cdots x_k \,(\text{mod}\, n).$$

Por fim, como $\text{mdc}\,(x_1 x_2 \ldots x_k, n) = 1$, segue da congruência acima e do item (f) da proposição 5.6 que $a^k \equiv 1 \,(\text{mod}\, n)$. ■

6.2 O conjunto quociente $\mathbb{Z}_n$

Examinemos, agora, o conjunto quociente

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \tag{6.5}$$

de $\mathbb{Z}$ pela relação de congruência módulo n. A proposição 5.6 nos permite introduzir em $\mathbb{Z}_n$ duas operações, às quais também nos referiremos como *adição* e *multiplicação* e que gozam de propriedades análogas às das operações usuais de adição e multiplicação de inteiros. De fato, temos o seguinte resultado fundamental.

Proposição 6.8. Em $\mathbb{Z}_n$, as operações

$$\overline{a} \oplus \overline{b} = \overline{a+b} \quad \text{e} \quad \overline{a} \odot \overline{b} = \overline{a \cdot b} \tag{6.6}$$

estão bem definidas, são comutativas, associativas e têm elementos neutros respectivamente iguais a $\overline{0}$ e $\overline{1}$. Ademais, $\odot$ é distributiva em relação a $\oplus$.

Prova. Inicialmente, temos de mostrar que as operações definidas por (6.6) estão bem definidas, no sentido de que os resultados de $\overline{a} \oplus \overline{b}$ e $\overline{a} \odot \overline{b}$ independem dos representantes escolhidos para as classes de congruência $\overline{a}$ e $\overline{b}$.

Para tanto, se $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d}$, então $a \equiv c \,(\text{mod}\, n)$ e $b \equiv d \,(\text{mod}\, n)$ e segue, da proposição 5.6, que

$$a + b \equiv c + d \,(\text{mod}\, n) \quad \text{e} \quad a \cdot b \equiv c \cdot d \,(\text{mod}\, n).$$

Mas isso é o mesmo que

$$\overline{a+b} = \overline{c+d} \quad \text{e} \quad \overline{a \cdot b} = \overline{c \cdot d},$$

de sorte que

$$\overline{a} \oplus \overline{b} = \overline{c} \oplus \overline{d} \quad \text{e} \quad \overline{a} \odot \overline{b} = \overline{c} \odot \overline{d}.$$

O que falta é mais simples. Por exemplo, para a comutatividade de $\oplus$, temos, a partir da comutatividade da adição de inteiros, que

$$\overline{a} \oplus \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} \oplus \overline{a};$$

analogamente, provamos que $\odot$ é comutativa e que $\oplus$ e $\odot$ são associativas, i.e., tais que

$$\overline{a} \oplus (\overline{b} \oplus \overline{c}) = (\overline{a} \oplus \overline{b}) \oplus \overline{c}$$

e

$$\overline{a} \odot (\overline{b} \odot \overline{c}) = (\overline{a} \odot \overline{b}) \odot \overline{c}.$$

A verificação dos elementos neutros também é imediata:

$$\overline{a} \oplus \overline{0} = \overline{a+0} = \overline{a} \quad \text{e} \quad \overline{a} \odot \overline{1} = \overline{a \cdot 1} = \overline{a}.$$

Por fim, a verificação da distributividade de $\odot$ em relação a $\oplus$ será deixada como exercício para o leitor (cf. problema 2). ■

À guisa de exemplo, mostramos, a seguir, as tábuas de adição e multiplicação em $\mathbb{Z}_6$:

Tábua de Adição em $\mathbb{Z}_6$

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

Tábua de Multiplicação em $\mathbb{Z}_6$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Sempre que não houver perigo de confusão, escreveremos simplesmente $+$ e $\cdot$, em vez de $\oplus$ e $\odot$, para denotar as operações de adição e multiplicação em $\mathbb{Z}_n$. Assim, o leitor deve permanecer atento para o fato de que, nas igualdades

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b},$$

os dois sinais $+$ e $\cdot$ denotam operações distintas: o primeiro sinal $+$ denota a operação de adição em $\mathbb{Z}_n$, ao passo que o segundo sinal $+$ denota a adição usual de inteiros (valendo uma observação análoga para os sinais $\cdot$).

A associatividade da adição de $\mathbb{Z}_n$ fornece imediatamente a *lei de cancelamento*

$$\overline{a} + \overline{b} = \overline{a} + \overline{c} \Rightarrow \overline{b} = \overline{c}.$$

De fato, se $\overline{a} + \overline{b} = \overline{a} + \overline{c}$, então

$$\overline{-a} + (\overline{a} + \overline{b}) = \overline{-a} + (\overline{a} + \overline{c})$$

e, daí,

$$(\overline{-a} + \overline{a}) + \overline{b} = (\overline{-a} + \overline{a}) + \overline{c}.$$

Mas, como $\overline{-a} + \overline{a} = \overline{-a+a} = \overline{0}$ e $\overline{0}$ é o elemento neutro da adição em $\mathbb{Z}_n$, temos, a partir da igualdade acima, que $\overline{b} = \overline{c}$.

Para a multiplicação de $\mathbb{Z}_n$, a lei de cancelamento é um pouco mais complicada. Temos, inicialmente, a definição a seguir.

Definição 6.9. Um elemento $\overline{a} \in \mathbb{Z}_n$ é uma **unidade** se existir $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

Assim como com conjuntos numéricos ordinários, as classes $\overline{\pm 1}$ são unidades em $\mathbb{Z}_n$, pois $\overline{\pm 1} \cdot \overline{\pm 1} = \overline{1}$. Por outro lado, a novidade em relação a $\mathbb{Z}$ é que pode haver outras unidades; por exemplo, em $\mathbb{Z}_9$ as classes $\overline{4}$ e $\overline{7}$ são unidades, uma vez que

$$\overline{4} \cdot \overline{7} = \overline{4 \cdot 7} = \overline{1} = \overline{7} \cdot \overline{4}.$$

Se $\overline{a} \in \mathbb{Z}_n$ é uma unidade, então temos a seguinte lei de cancelamento em relação à multiplicação:

$$\overline{a} \cdot \overline{c} = \overline{a} \cdot \overline{d} \Rightarrow \overline{c} = \overline{d}.$$

De fato, tomando $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$ (e, portanto, $\overline{b} \cdot \overline{a} = \overline{1}$ também), segue de $\overline{a} \cdot \overline{c} = \overline{a} \cdot \overline{d}$ que

$$\overline{b} \cdot (\overline{a} \cdot \overline{c}) = \overline{b} \cdot (\overline{a} \cdot \overline{d}).$$

Então, a associatividade da multiplicação fornece

$$(\overline{b} \cdot \overline{a}) \cdot \overline{c} = (\overline{b} \cdot \overline{a}) \cdot \overline{d}$$

ou, ainda, $\overline{1} \cdot \overline{c} = \overline{1} \cdot \overline{d}$. Mas isso é o mesmo que $\overline{c} = \overline{d}$, conforme desejado.

Em particular, se $\overline{a} \in \mathbb{Z}_n$ é uma unidade, então o elemento $\overline{b} \in \mathbb{Z}_n$ cuja existência é garantida pela definição 6.9 é único, pois se

$$\overline{a} \cdot \overline{b} = \overline{1} = \overline{a} \cdot \overline{c},$$

então a lei do cancelamento para a multiplicação garante que $\overline{b} = \overline{c}$. Dizemos, portanto, que tal $\overline{b} \in \mathbb{Z}_n$ é o **inverso multiplicativo** de $\overline{a}$.

A proposição a seguir caracteriza todas as unidades de $\mathbb{Z}_n$.

Proposição 6.10. Uma classe de congruência $\overline{a} \in \mathbb{Z}_n$ é uma unidade em $\mathbb{Z}_n$ se e só se $\text{mdc}\,(a, n) = 1$. Em particular, $\mathbb{Z}_n$ possui exatamente $\varphi(n)$ unidades distintas.

Prova. Por definição, $\overline{a} \in \mathbb{Z}_n$ é uma unidade se, e só se, existir $\overline{b} \in \mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$, i.e., tal que $\overline{ab} = \overline{1}$ ou, ainda,

$$ab \equiv 1 \pmod{n}.$$

Portanto, $\overline{a}$ é uma unidade em $\mathbb{Z}_n$ se, e só se, $a \in \mathbb{Z}$ for um invertível módulo n. Mas, pela proposição 5.23, tal ocorre se, e só se, $\text{mdc}\,(a, n) = 1$.

Para o que falta, basta observar que, como $\mathbb{Z}_n = \{\overline{1}, \overline{2}, \ldots, \overline{n}\}$, o conjunto das unidades de $\mathbb{Z}_n$ coincide com o conjunto das classes $\overline{a}$ tais que $1 \leq a \leq n$ e $\text{mdc}\,(a, n) = 1$. Mas, uma vez que tal conjunto tem $\varphi(n)$ elementos, nada mais há a fazer. ■

Chegamos ao caso de maior interesse.

Corolário 6.11. Se p é primo, então todo elemento em $\mathbb{Z}_p \setminus \{\overline{0}\}$ é uma unidade.

Prova. Pela proposição anterior, basta mostrar que, se $\overline{a} \neq \overline{0}$ em $\mathbb{Z}_p$, então $\text{mdc}\,(a, p) = 1$. Mas, $\overline{a} \neq \overline{0}$ é o mesmo que $a \not\equiv 0 \pmod{p}$ ou, ainda, $p \nmid a$, e a prova do lema 1.40 garante que $p \nmid a$ se, e só se, $\text{mdc}\,(a, p) = 1$. ■

Em termos das operações aritméticas de adição, subtração, multiplicação e divisão, o corolário acima nos permite colocar $\mathbb{Z}_p$, p primo em pé de igualdade com os conjuntos numéricos $\mathbb{Q}$ e $\mathbb{R}$ (e, após o capítulo 1 do volume 6, também com o conjunto $\mathbb{C}$ dos números complexos). Mais precisamente, em $\mathbb{Z}_n$ (para todo $n > 1$, não somente n primo) podemos definir uma operação $-$, a qual chamaremos *subtração*, análoga à subtração ordinária de números reais, pondo

$$\overline{a} - \overline{b} = \overline{a - b}$$

(cf. problema 3). Por outro lado, restrinjamo-nos agora ao caso em que $n = p$, um número primo; se, para $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$, convencionarmos escrever $\overline{a}^{-1}$ para denotar o inverso multiplicativo de $\overline{a}$ (i.e., se denotarmos por $\overline{a}^{-1}$ a classe $\overline{b} \in \mathbb{Z}_p$ cuja existência é garantida pela definição 6.9), então

$$\overline{a} \cdot \overline{a}^{-1} = \overline{1};$$

ademais, se $\overline{a} \cdot \overline{b} = \overline{c}$, com $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_p$ e $\overline{b} \neq \overline{0}$, então é imediato verificar que

$$\overline{a} = \overline{c} \cdot \overline{b}^{-1}.$$

Portanto, podemos definir em $\mathbb{Z}_p$ uma operação de divisão de forma análoga à divisão usual entre números reais (resp. complexos, cf. capítulo 1 do volume 6), i.e., pondo, para $\overline{b} \in \mathbb{Z}_p \setminus \{\overline{0}\}$ e $\overline{a} \in \mathbb{Z}_p$,

$$\overline{a} \div \overline{b} = \overline{a} \cdot \overline{b}^{-1}.$$

Problemas – Seção 6.2

1. Escreva as tábuas de adição e multiplicação de $\mathbb{Z}_5$ e $\mathbb{Z}_7$.

2. * Prove que, em $\mathbb{Z}_n$, a multiplicação é distributiva em relação à adição. Mais precisamente, mostre que

$$\overline{a} \cdot (\overline{b} + \overline{c}) = (\overline{a} \cdot \overline{b}) + (\overline{a} \cdot \overline{c}),$$

para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$.

3. * Prove que a operação de subtração em $\mathbb{Z}_n$ está bem definida.

4. Em $\mathbb{Z}_{12}$, obtenha todas as unidades que são iguais a seus inversos multiplicativos.

5. Fixados m, n inteiros, sendo $n > 1$, mostre que a operação de *multiplicação por* m em $\mathbb{Z}_n$, dada por $m \cdot \overline{a} = \overline{m \cdot a}$ está bem definida e é tal que

$$m \cdot (\overline{a} + \overline{b}) = m \cdot \overline{a} + m \cdot \overline{b} \;\text{ e }\; (m_1 + m_2) \cdot \overline{a} = m_1 \cdot \overline{a} + m_2 \cdot \overline{a},$$

para todos $m, m_1, m_2 \in \mathbb{Z}$ e $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

6. Se $n > 1$ não é primo, mostre que $\mathbb{Z}_n$ possui *divisores de zero*, i.e., que existem $\overline{a}, \overline{b} \in \mathbb{Z}_n$, tais que $\overline{a}, \overline{b} \neq \overline{0}$, mas $\overline{a} \cdot \overline{b} = \overline{0}$. Mostre ainda que, se p é um número primo, então $\mathbb{Z}_p$ não possui divisores de zero.

7. Sejam dados a e n inteiros, sendo $n > 1$. Mostre que, em $\mathbb{Z}_n$, a equação $\overline{a} \cdot x = \overline{b}$ tem solução para todo $\overline{b} \in \mathbb{Z}_n$ se, e só se, $\overline{a}$ for uma unidade em $\mathbb{Z}_n$. Nesse caso, mostre que a solução $x \in \mathbb{Z}_n$ é única, sendo dada por $x = \overline{a}^{-1} \cdot \overline{b}$.

CAPÍTULO 7

Raízes Primitivas e Resíduos Quadráticos

Neste último capítulo, retomamos a análise da congruência

$$a^k \equiv 1 \pmod{n},$$

concentrando-nos em dois problemas distintos, descritos brevemente a seguir. Por um lado, já sabemos pelo teorema de Euler que, se $\text{mdc}\,(a,n) = 1$, então tal congruência sempre é satisfeita para $k = \varphi(n)$, onde φ denota a função de Euler; por outro lado, fixado $a \in \mathbb{Z}$ primo com n, nada sabemos ainda sobre se tal valor de k é o menor possível, e um dos resultados centrais deste capítulo é a caracterização dos números inteiros a relativamente primos com n, ditos as *raízes primitivas* módulo n, tais que o valor mínimo de k é $k = \varphi(n)$.

Um segundo problema que queremos considerar aqui impõe uma importante mudança de ponto de vista em relação à congruência acima. Em vez de fixarmos a base a e procurarmos os valores $k \in \mathbb{N}$ para os

quais a congruência tenha solução, fixamos $k \in \mathbb{N}$ e procuramos os valores $a \in \mathbb{Z}$ que resolvem a congruência em questão. De fato, dado o caráter elementar destas notas, restringimo-nos ao caso $k = 2$, quando os $a \in \mathbb{Z}$ que resolvem a congruência são os *resíduos quadráticos* módulo n.

Como subproduto da teoria desenvolvida, provamos mais um famoso teorema de Fermat, que desta feita caracteriza os números naturais que podem ser escritos como a soma dos quadrados de dois inteiros.

7.1 Ordem módulo n

Sejam a, n inteiros tais que $n > 1$ e $\text{mdc}\,(a, n) = 1$. Sabemos, pelo teorema de Euler 5.19, que sempre existe um natural k tal que $a^k \equiv 1 \pmod n$, qual seja, $k = \varphi(n)$. Contudo, não há nada que garanta ser $\varphi(n)$ o menor dentre tais naturais k; por exemplo, $2^3 \equiv 1 \pmod 7$ mas $\varphi(7) = 6$. Essas considerações motivam a definição a seguir.

Definição 7.1. Dados a e n inteiros primos entre si, com $n > 1$, a **ordem** de a, módulo n, denotada $\text{ord}_n(a)$, é o menor $h \in \mathbb{N}$ para o qual

$$a^h \equiv 1 \pmod n.$$

Das considerações acima, é imediato que

$$\text{ord}_n(a) \leq \varphi(n),$$

nem sempre ocorrendo a igualdade. A proposição a seguir estabelece algumas propriedades elementares do número $\text{ord}_n(a)$.

Proposição 7.2. Sejam $a, n \in \mathbb{Z}$, com $n > 1$ e $\text{mdc}\,(a, n) = 1$.

(a) Se $\text{ord}_n(a) = h$, então os inteiros $1, a, a^2, \ldots, a^{h-1}$ são dois a dois incongruentes, módulo n. Em particular, se $\text{ord}_n(a) = \varphi(n)$, então o conjunto $\{1, a, a^2, \ldots, a^{\varphi(n)-1}\}$ é um SCI módulo n.

(b) $a^k \equiv 1 \pmod n \Leftrightarrow \text{ord}_n(a) \mid k$. Em particular, $\text{ord}_n(a) \mid \varphi(n)$.

Prova.
(a) Se existissem $0 \leq k < l < h$ tais que $a^l \equiv a^k \pmod n$, o item (f) da proposição 5.6 daria $a^{l-k} \equiv 1 \pmod n$, com $0 < l - k < h$. Mas isso seria uma contradição à minimalidade de h.

Para o que falta, basta ver que, se $\text{ord}_n(a) = \varphi(n)$, então o conjunto $\{1, a, a^2, \ldots, a^{\varphi(n)-1}\}$ tem $\varphi(n)$ inteiros primos com n e dois a dois incongruentes módulo n, logo é um SCI módulo n.

(b) Seja $\text{ord}_n(a) = h$, de sorte que, em particular, $a^h \equiv 1 \pmod n$. Se $k = hl$, então

$$a^k = a^{hl} = (a^h)^l \equiv 1^l = 1 \pmod n.$$

Reciprocamente, seja k um natural tal que $a^k \equiv 1 \pmod n$. Pelo algoritmo da divisão, existem inteiros q e r, com $0 \leq r < h$, tais que $k = qh + r$. Assim, temos

$$1 \equiv a^k = a^{qh+r} = (a^h)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod n.$$

Se $r > 0$, temos que r é um expoente positivo, menor que h e tal que $a^r \equiv 1 \pmod n$, contradizendo a minimalidade de h. Logo, $r = 0$ e então $h \mid k$, i.e., $\text{ord}_n(a) \mid k$.

Por fim, a relação $\text{ord}_n(a) \mid \varphi(n)$ segue da primeira parte do item (b), juntamente com o teorema de Euler 5.19. ■

Exemplo 7.3. Calcule as ordens de 2 módulo 17 e de 7 módulo 10.

Solução. Se $h = \text{ord}_{17}(2)$, então $h \mid \varphi(17) = 16$, de sorte que $h = 1$, 2, 4, 8 ou 16. Evidentemente $h \neq 1, 2$; também, $2^4 \equiv -1 \pmod{17}$, de modo que $h \neq 4$. Por outro lado, $2^8 = (2^4)^2 \equiv (-1)^2 \equiv 1 \pmod{17}$ e, daí, $h = 8$.

Se $h = \text{ord}_{10}(7)$, então $h \mid \varphi(10) = 4$, de maneira que $h = 1$, 2 ou 4. Evidentemente, $h \neq 1$; mas, como $7^2 \equiv -1 \pmod{10}$, também temos $h \neq 2$. Logo, $h = 4$. ■

Vejamos, agora, como a proposição 7.2 pode ser aplicada à resolução de problemas interessantes.

Exemplo 7.4. Se p é um primo ímpar, prove que todos os fatores primos de $2^p - 1$ são da forma $2kp + 1$, para algum $k \in \mathbb{N}$.

Prova. Se q é um primo que divide $2^p - 1$, então q é ímpar e $2^p \equiv 1 \pmod{q}$. Segue do item (b) da proposição anterior que $\text{ord}_q(2) \mid p$ e, daí, $\text{ord}_q(2) = 1$ ou p. Mas, se $\text{ord}_q(2) = 1$, então $q = 1$, o que é um absurdo; logo, $\text{ord}_q(2) = p$.

Por outro lado, segue do pequeno teorema de Fermat que $2^{q-1} \equiv 1 \pmod{q}$, de sorte que, novamente pelo item (b) da proposição anterior, temos

$$p = \text{ord}_q(2) \mid (q-1).$$

Mas como q é ímpar, deve existir $k \in \mathbb{N}$ tal que $q - 1 = 2kp$. ■

A proposição a seguir estabelece mais algumas propriedades úteis da ordem módulo n de inteiros, as quais serão de grande utilidade no que segue.

Proposição 7.5. Sejam a e n inteiros primos entre si, com $n > 1$.

(a) $\text{ord}_n(a) = \text{ord}_n(a+n)$.

(b) Se $m > 1$ é um natural tal que $m \mid n$, então $\text{ord}_m(a) \mid \text{ord}_n(a)$.

(c) Se $\text{ord}_n(a) = h$ e $k \in \mathbb{N}$, então $\text{ord}_n(a^k) = \frac{h}{\text{mdc}\,(h,k)}$.

(d) Se $k \in \mathbb{N}$, então $\text{ord}_n(a^k) = \text{ord}_n(a) \Leftrightarrow \text{mdc}\,(\text{ord}_n(a), k) = 1$.

(e) Se $\text{ord}_n(a) = h$, então o conjunto $\{a, a^2, \ldots, a^h\}$ tem exatamente $\varphi(h)$ elementos com ordem h módulo n.

Prova.
(a) Segue de $a \equiv a + n \pmod{n}$ que $a^k \equiv (a+n)^k \pmod{n}$, para todo $k \in \mathbb{N}$. Em particular, $a^k \equiv 1 \pmod{n}$ se, e só se, $(a+n)^k \equiv 1 \pmod{n}$ e, daí, a e $a + n$ têm ordens iguais, módulo n.

(b) Como $m \mid n$, o item (g) da proposição 5.6 garante que, se $a^k \equiv 1 \pmod{n}$, então $a^k \equiv 1 \pmod{m}$. Em particular, como $a^k \equiv 1 \pmod{n}$ quando $k = \text{ord}_n(a)$, temos que

$$a^{\text{ord}_n(a)} \equiv 1 \pmod{m}.$$

O item (b) da proposição 7.2 garante, agora, que $\text{ord}_m(a) \mid \text{ord}_n(a)$.

(c) Seja $d = \text{mdc}\,(h,k)$. Pelo item (b) da proposição 7.2, temos

$$\begin{aligned} (a^k)^j \equiv 1 \pmod{n} \;\; &\Leftrightarrow \;\; a^{kj} \equiv 1 \pmod{n} \Leftrightarrow h \mid kj \\ &\Leftrightarrow \;\; \frac{h}{d} \mid \frac{k}{d} \cdot j \Leftrightarrow \frac{h}{d} \mid j, \end{aligned}$$

onde, na última equivalência, utilizamos o item (a) da proposição 1.21, juntamente com o fato de $\text{mdc}\left(\frac{h}{d}, \frac{k}{d}\right) = 1$. A partir daí, é imediato que

$$\text{ord}_n(a^k) = \frac{h}{d} = \frac{h}{\text{mdc}\,(h,k)}.$$

(d) Segue claramente de (c).

(e) Pelo item (d), o número de expoentes $1 \leq k \leq h$ tais que a^k tem ordem h módulo n é igual ao número de tais expoentes relativamente primos com h, i.e., é igual a $\varphi(h)$. ■

Problemas – Seção 7.1

1. Calcule $\text{ord}_7(2)$, $\text{ord}_{11}(2)$ e $\text{ord}_{15}(7)$.

2. Prove que, para todo inteiro positivo n, o número $2^{3^n}+1$ não é múltiplo de 17.

3. Sejam a e n inteiros primos entre si, com $n > 2$. Se existe um natural k tal que $a^k \equiv -1 \pmod n$, prove que $\text{ord}_n(a)$ é par.

4. (Putnam.) Ache todos os $n \in \mathbb{N}$ tais que $n \mid (2^n - 1)$.

5. (Turquia.) Para cada $n \in \mathbb{N}$, prove que $n!$ divide o número

$$\prod_{j=0}^{n-1}(2^n - 2^j).$$

6. Dado um natural $n > 2$, rotulamos os vértices de um $2n$–ágono regular $\mathcal{P}$ como $1, 2, 3, \ldots, n, -n, -(n-1), \ldots, -3, -2, -1$, sucessivamente e no sentido horário. A seguir, marcamos os vértices de $\mathcal{P}$ da seguinte maneira: no primeiro passo, marcamos o vértice 1; por outro lado, se k_i foi o vértice marcado no i–ésimo passo, então, no $(i+1)$–ésimo passo, marcamos o vértice que se encontra a $|k_i|$ vértices do vértice k_i, no sentido horário se $k_i > 0$ e no sentido anti-horário se $k_i < 0$. Este procedimento continua até marcarmos um vértice já marcado em um passo anterior. Seja $f(n)$ o número de vértices não marcados ao final deste processo.

   (a) Se $f(n) = 0$, prove que $2n + 1$ é um primo ímpar.

   (b) Calcule $f(1997)$.

7.2 Raízes primitivas

Dados a, n inteiros tais que $n > 1$ e $\text{mdc}\,(a, n) = 1$, nesta seção estaremos particularmente interessados no caso em que $\text{ord}_n(a) = \varphi(n)$. Tal caso é tão importante que o isolamos na definição a seguir.

Definição 7.6. Sejam a, n inteiros tais que $n > 1$ e $\text{mdc}\,(a, n) = 1$. Dizemos que a é uma **raiz primitiva**, módulo n, se $\text{ord}_n(a) = \varphi(n)$.

Vejamos alguns exemplos.

Exemplos 7.7.

(a) Como $2^1 \equiv 2 \pmod 3$ e $\varphi(3) = 2$, segue que $\text{ord}_3(2) = 2 = \varphi(3)$, i.e., 2 é raiz primitiva módulo 3. Cálculos análogos garantem que 2 também é raiz primitiva módulo 5.

(b) Módulo 7 temos $2^1 \equiv 2$, $2^2 \equiv 4$ e $2^3 \equiv 1$. Portanto, $\text{ord}_7(2) = 3 < 6 = \varphi(7)$, e segue que 2 não é raiz primitiva módulo 7.

O principal resultado desta seção é a caracterização dos módulos n que possuem raízes primitivas. Mais precisamente, mostraremos que um inteiro $n > 1$ possui uma raiz primitiva se, e só se, $n = 2$, 4, p^k ou $2p^k$, onde p é um primo ímpar. Calculemos, inicialmente, quantas podem ser as raízes primitivas duas a duas incongruentes módulo n.

Proposição 7.8. Se um inteiro $n > 1$ tem uma raiz primitiva, a digamos, então toda raiz primitiva módulo n é congruente a um dos elementos do conjunto

$$\{a^k;\ 1 \le k \le \varphi(n) \text{ e } \text{mdc}\,(\varphi(n), k) = 1\}.$$

Em particular, n tem exatamente $\varphi(\varphi(n))$ raízes primitivas, duas a duas incongruentes módulo n.

Prova. A segunda parte segue da primeira, pela definição da função φ de Euler: o número de expoentes $1 \leq k \leq \varphi(n)$ tais que k é primo com $\varphi(n)$ é exatamente $\varphi(\varphi(n))$.

Para a primeira parte, sendo a uma raiz primitiva módulo n temos que $\text{ord}_n(a) = \varphi(n)$ e $A = \{a, a^2 \ldots, a^{\varphi(n)}\}$ é um SCI módulo n. Portanto, qualquer raiz primitiva módulo n é congruente, módulo n, a um dos elementos de A, de maneira que basta ver quais elementos de A têm ordem (módulo n) igual a $\varphi(n)$. Mas, pelo item (d) da proposição 7.5, para $1 \leq k \leq \varphi(n)$ temos

$$\text{ord}_n(a^k) = \varphi(n) \Leftrightarrow \text{mdc}\,(\varphi(n), k) = 1.$$

■

Exemplo 7.9. O exemplo 7.7 garante que 2 é raiz primitiva módulo 5. Como $\varphi(5) = 4$, a proposição acima ensina que um conjunto de raízes primitivas módulo 5 duas a duas incongruentes é

$$\{2^k;\ 1 \leq k \leq 4 \text{ e } \text{mdc}\,(4, k) = 1\} = \{2, 2^3\}.$$

Portanto, módulo 5 as raízes primitivas duas a duas incongruentes são 2 e 3 (uma vez que $8 \equiv 3 \pmod 5$).

Prosseguimos, agora, na direção da caracterização dos inteiros que possuem raízes primitivas. Comecemos com uma condição necessária.

Teorema 7.10. Se $n > 1$ é um inteiro que possui raízes primitivas, então $n = 2, 4, p^k$ ou $2p^k$, onde p é um primo ímpar e k é um natural.

Prova. Note, inicialmente, que os inteiros $n > 1$ que não são de uma das formas do enunciado são ou da forma $n = bc$, com $b, c > 2$ inteiros primos entre si, ou da forma $n = 2^k$, com $k > 2$ inteiro. Basta, pois, mostrarmos que tais inteiros n não possuem raízes primitivas, coisa que faremos mostrando que todo inteiro a primo com n satisfaz

$\text{ord}_n(a) < \varphi(n)$.

(i) $n = bc$, com $b, c > 2$ primos entre si: como b e c são primos entre si, temos $\varphi(n) = \varphi(bc) = \varphi(b)\varphi(c)$. Por outro lado, o fato de que $b, c > 2$ garante (cf. problema 19, página 88) que $\varphi(b)$ e $\varphi(c)$ são números pares. Se a é um inteiro qualquer primo com n, então a é primo com b e com c e, pelo teorema de Euler,

$$a^{\varphi(n)/2} = \left(a^{\varphi(b)}\right)^{\varphi(c)/2} \equiv 1^{\varphi(c)/2} \equiv 1 \pmod b$$

e

$$a^{\varphi(n)/2} = \left(a^{\varphi(c)}\right)^{\varphi(b)/2} \equiv 1^{\varphi(b)/2} \equiv 1 \pmod c.$$

Portanto, o item (h) da proposição 5.6 garante que $a^{\varphi(n)/2} \equiv 1 \pmod n$; em particular,

$$\text{ord}_n(a) \leq \frac{\varphi(n)}{2} < \varphi(n)$$

e, daí, a não é raiz primitiva módulo n.

(ii) $n = 2^k$, com $k > 2$: seja a um inteiro ímpar (i.e., primo com 2). Se mostrarmos que

$$a^{2^{k-2}} \equiv 1 \pmod{2^k},$$

teremos

$$\text{ord}_{2^k}(a) \leq 2^{k-2} < 2^{k-1} = \varphi(2^k),$$

e a não será raiz primitiva módulo 2^k. Para o que falta, façamos indução sobre k: o caso inicial $k = 3$ segue da proposição 5.9, uma vez que $a^2 \equiv 1 \pmod 8$ para a ímpar. Suponha que já provamos que, para algum inteiro $k \geq 3$, existe $q \in \mathbb{N}$ tal que $a^{2^{k-2}} = 2^k q + 1$; então

$$\begin{aligned} a^{2^{k-1}} &= \left(a^{2^{k-2}}\right)^2 = (2^k q + 1)^2 = 2^{2k} q^2 + 2^{k+1} q + 1 \\ &= 2^{k+1}(2^{k-1} q^2 + q) + 1 \equiv 1 \pmod{2^{k+1}}, \end{aligned}$$

conforme desejado. ■

Resta estabelecer a recíproca do teorema acima, qual seja, que os números 2, 4, p^k e $2p^k$, com p primo ímpar e $k \in \mathbb{N}$, possuem raízes primitivas. É claro que 1 é raiz primitiva módulo 2 e 3 é raiz primitiva módulo 4. O restante desta seção é devotado à análise dos demais casos.

A proposição a seguir garante que basta nos preocuparmos com os números da forma p^k.

Proposição 7.11. Se p é um primo ímpar e $a \in \mathbb{Z}$ é uma raiz primitiva módulo p^k, então a ou $a + p^k$ também é raiz primitiva módulo $2p^k$.

Prova. Seja $h = \text{ord}_{2p^k}(a)$. Se a for ímpar, então a é primo com $2p^k$. Nesse caso, usando o item (b) da proposição 7.5, juntamente com o fato de ser $\text{ord}_{p^k}(a) = \varphi(p^k)$, obtemos

$$\varphi(p^k) = \text{ord}_{p^k}(a) \mid h = \text{ord}_{2p^k}(a) \mid \varphi(2p^k) = \varphi(p^k),$$

onde, na última igualdade, utilizamos o fato de p ser um primo ímpar; logo, $\text{ord}_{2p^k}(a) = \varphi(2p^k)$ e a é raiz primitiva módulo $2p^k$.

Se a for par, troque a por $a + p^k$ no início e argumente como acima. ■

Completaremos a prova da recíproca do teorema 7.10 (i.e., a análise do caso p^k), em duas etapas. Antes, contudo, precisamos do seguinte

Lema 7.12. Seja p um primo ímpar. Se a é uma raiz primitiva módulo p^2, então, para $k \geq 1$ inteiro, temos $a^{\varphi(p^k)} = b_k p^k + 1$, com $b_k \in \mathbb{Z}$ tal que $p \nmid b_k$.

Prova. Façamos indução sobre $k \geq 1$. O pequeno teorema de Fermat nos dá $a^{p-1} = b_1 p + 1$ para algum $b_1 \in \mathbb{Z}$. Se p dividisse b_1, teríamos $a^{p-1} \equiv 1 \pmod{p^2}$ e, daí, $\text{ord}_{p^2}(a) \leq p - 1 < \varphi(p^2)$, contrariando o fato de a ser uma raiz primitiva módulo p^2.

Suponha que, para um certo $k \geq 1$, tenhamos $a^{\varphi(p^k)} = b_k p^k + 1$, tal que $p \nmid b_k$. A fórmula do binômio de Newton nos dá, então,

$$\begin{aligned} a^{\varphi(p^{k+1})} &= \left(a^{\varphi(p^k)}\right)^p = (1 + b_k p^k)^p \\ &= 1 + b_k p^{k+1} + \sum_{j=2}^{p-1} \binom{p}{j} b_k^j p^{jk} + b_k^p p^{pk}. \end{aligned}$$

Pelo exemplo 1.41, para $1 \leq j \leq p - 1$ existe $c_k \in \mathbb{N}$ tal que $\binom{p}{j} = pc_k$. Portanto, a última expressão acima fornece

$$\begin{aligned} a^{\varphi(p^{k+1})} &= 1 + b_k p^{k+1} + \sum_{j=2}^{p-1} c_k b_k^j p^{jk+1} + b_k^p p^{pk} \\ &= 1 + b_k p^{k+1} + \left(\sum_{j=2}^{p-1} c_k b_k^j p^{(j-1)k-1} + b_k^p p^{(p-1)k-2}\right) p^{k+2}. \end{aligned}$$

Denotando por t a expressão acima entre parênteses e observando que $t \in \mathbb{Z}$, segue finalmente que

$$a^{\varphi(p^{k+1})} = 1 + b_k p^{k+1} + tp^{k+2} = 1 + (b_k + tp)p^{k+1}.$$

Mas, como $p \nmid b_k$, fazendo $b_{k+1} = b_k + tp$ obtemos $a^{\varphi(p^{k+1})} = b_{k+1}p^{k+1} + 1$, tal que $p \nmid b_{k+1}$. ■

Podemos finalmente cumprir o primeiro dos dois passos necessários à demonstração da existência de raízes primitivas módulo p^k, com p primo ímpar.

Teorema 7.13. Seja p um primo ímpar e a um inteiro primo com p.

(a) Se a for uma raiz primitiva módulo p, então a ou $a + p$ é raiz primitiva módulo p^2.

(b) Se a for uma raiz primitiva módulo p e módulo p^2, então a é raiz primitiva módulo p^k, para todo inteiro $k \geq 1$.

Prova.
(a) Segue do item (a) da proposição 7.5 e de nossas hipóteses que $\mathrm{ord}_p(a+p) = \mathrm{ord}_p(a) = p-1$; por outro lado, o item (b) da proposição 7.2 garante que

$$\mathrm{ord}_{p^2}(a+p),\ \mathrm{ord}_{p^2}(a) \mid \varphi(p^2) = p(p-1),$$

ao passo que o item (b) da proposição 7.5 garante que

$$p-1 = \mathrm{ord}_p(a) \mid \mathrm{ord}_{p^2}(a) \quad \text{e} \quad p-1 = \mathrm{ord}_p(a+p) \mid \mathrm{ord}_{p^2}(a+p).$$

Portanto, $\mathrm{ord}_{p^2}(a) = p-1$ ou $p(p-1)$, o mesmo sendo válido para $\mathrm{ord}_{p^2}(a+p)$, e basta mostrarmos que

$$\mathrm{ord}_{p^2}(a) = p-1 \Rightarrow \mathrm{ord}_{p^2}(a+p) \neq p-1.$$

Mas, se $a^{p-1} \equiv 1 \pmod{p^2}$, então, módulo p^2, temos

$$\begin{aligned}(a+p)^{p-1} &= a^{p-1} + (p-1)pa^{p-2} + \sum_{j=2}^{p-1}\binom{p-1}{j}p^j a^{p-1-j}\\ &\equiv a^{p-1} + (p-1)pa^{p-2}\\ &\equiv 1 - pa^{p-2} \not\equiv 1,\end{aligned}$$

uma vez que $p \nmid a$.

(b) Suponha que a é uma raiz primitiva módulo p e módulo p^2 e provemos, por indução sobre k, que a é uma raiz primitiva módulo p^k, para todo $k \geq 1$. Os casos $k = 1$ e $k = 2$ são nossas hipóteses. Suponha, pois, que já provamos ser a uma raiz primitiva módulo p^k, para um certo $k \geq 2$.

Os itens (b) das proposições 7.2 e 7.5 nos dão

$$\varphi(p^k) = \mathrm{ord}_{p^k}(a) \mid \mathrm{ord}_{p^{k+1}}(a) \mid \varphi(p^{k+1}) = p\varphi(p^k),$$

de sorte que

$$\mathrm{ord}_{p^{k+1}}(a) = \varphi(p^k) \text{ ou } \varphi(p^{k+1}).$$

Para o que falta, como a é raiz primitiva módulo p^2, o lema anterior nos dá $a^{\varphi(p^k)} = b_k p^k + 1$, com $b_k \in \mathbb{Z}$ tal que $p \nmid b_k$; em particular,

$$a^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}},$$

de maneira que $\mathrm{ord}_{p^{k+1}}(a) \neq \varphi(p^k)$. ■

O teorema 7.13 nos coloca numa posição bastante boa. De fato, se mostrarmos que o primo ímpar p possui uma raiz primitiva, a digamos, então $a+p$ também o será (pelo item (a) da proposição 7.5); portanto, pelo item (a) do teorema anterior, podemos supor que a é raiz primitiva módulo p e módulo p^2, após o quê o item (b) do mesmo resultado garante que a é raiz primitiva módulo p^k, para todo inteiro $k \geq 1$. Vejamos um exemplo.

Exemplo 7.14. Prove que 2 é raiz primitiva módulos 3^k e 5^k, para todo $k \in \mathbb{N}$.

Prova. Segue do exemplo 7.7 e do teorema anterior que basta mostrarmos que 2 é raiz primitiva módulos 9 e 25. Verifiquemos que 2 é raiz primitiva módulo 9, sendo o caso do módulo 25 análogo: como $\varphi(9) = 6$, segue que $\mathrm{ord}_9(2) \mid 6$; mas, uma vez que nenhum dos números 2^1, 2^2 ou 2^3 é múltiplo de 9, segue que $\mathrm{ord}_9(2) = 6 = \varphi(9)$. ■

Para concluirmos a recíproca do teorema 7.10, resta apenas mostrar que primos ímpares possuem raízes primitivas. Como não é possível darmos uma prova desta afirmação com o material de que dispomos até o momento, adiaremos a apresentação de uma demonstração para a seção 7.3 do volume 6 (cf. teorema 7.20 de lá).

Finalizamos esta seção com dois exemplos que mostram a força dos resultados aqui desenvolvidos.

Exemplo 7.15. Se p é primo e $n \in \mathbb{N}$, prove que

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p}, & \text{se } (p-1) \nmid n \\ -1 \pmod{p}, & \text{se } (p-1) \mid n \end{cases}.$$

Prova. Se $(p-1) \mid n$, digamos $n = (p-1)k$, o pequeno teorema de Fermat nos dá, para $1 \leq a \leq p-1$, que

$$a^n = a^{(p-1)k} \equiv 1^k = 1 \pmod{p}$$

e, daí,

$$1^n + 2^n + \cdots + (p-1)^n \equiv \underbrace{1 + 1 + \cdots + 1}_{p-1} \equiv -1 \pmod{p}.$$

Se $(p-1) \nmid n$, seja a uma raiz primitiva módulo p. Como o conjunto $\{a, a^2, \ldots, a^{p-1}\}$ é um SCI, módulo p, concluímos que os números a, a^2, $\ldots$, a^{p-1} são, módulo p, congruentes, em alguma ordem, aos números $1, 2, \ldots, p-1$. Portanto (ainda módulo p), temos

$$1^n + 2^n + \cdots + (p-1)^n \equiv a^n + a^{2n} + \cdots + a^{(p-1)n} = \frac{a^{pn} - a^n}{a^n - 1}.$$

Agora, segue do pequeno teorema de Fermat que

$$a^{pn} - a^n = (a^p)^n - a^n \equiv a^n - a^n \equiv 0 \pmod{p};$$

por outro lado, uma vez que $\text{ord}_p(a) = p-1$ e $(p-1) \nmid n$, o item (b) da proposição 7.2 garante que $p \nmid (a^n - 1)$. Logo, $p \mid \frac{a^{pn}-a^n}{a^n-1}$, conforme desejado. ■

Exemplo 7.16 (IMO). Ache todos os $n \in \mathbb{N}$ tais que n^2 divide $2^n + 1$.

Solução. É claro que um tal n deve ser ímpar e que $n = 1$ é um valor possível. Seja, pois, $n > 1$ um natural satisfazendo as condições do enunciado e escreva $n = p^k q$, onde p é o menor primo que divide n e

$k \in \mathbb{N}$ é o expoente de p na decomposição canônica de n em fatores primos. Então $\text{mdc}\,(p, q) = 1$ e

$$\frac{2^n + 1}{n^2} \in \mathbb{N} \Rightarrow \frac{2^n + 1}{p^{2k}} \in \mathbb{N}.$$

Pelo pequeno teorema de Fermat, temos $2^p \equiv 2 \pmod{p}$ e, a partir daí, uma fácil indução garante que $2^{p^k} \equiv 2 \pmod{p}$. Assim, módulo p temos

$$0 \equiv 2^n + 1 = 2^{p^k q} + 1 \equiv 2^q + 1,$$

de modo que $2^{2q} \equiv 1 \pmod{p}$. Sendo $t = \text{ord}_p(2)$, segue, daí, que t divide $2q$ e (pelo pequeno teorema de Fermat) $t \mid (p-1)$; logo, $t \mid \text{mdc}\,(2q, p-1)$. Mas, como os fatores primos de q são maiores que p, isto força que $t = 2$ e, por conseguinte, $t = 2$ e $p = 3$. Portanto,

$$\frac{2^n + 1}{n^2} = \frac{2^{3^k q} + 1}{3^{2k} q^2} \in \mathbb{N}, \tag{7.1}$$

o que acarreta sucessivamente $2^{3^k q} \equiv -1 \pmod{3^{2k}}$ e

$$2^{2 \cdot 3^k q} \equiv 1 \pmod{3^{2k}}.$$

Como já mostramos (cf. exemplo 7.14) que 2 é raiz primitiva módulo 3^{2k}, segue da congruência acima que

$$2 \cdot 3^{2k-1} = \varphi(3^{2k}) = \text{ord}_{3^{2k}}(2) \mid 2 \cdot 3^k q$$

e, assim, $3^{k-1} \mid q$. Mas, como $p = 3$ e $\text{mdc}\,(3, q) = 1$, devemos ter $k = 1$. Assim, $n = 3q$ e, por (7.1),

$$\frac{8^q + 1}{q^2} \in \mathbb{N}.$$

Suponha $q > 1$, e seja w o menor fator primo de q, digamos $q = w^l v$, onde $v \in \mathbb{N}$ e l é o expoente de w na decomposição canônica de q em

fatores primos. Novamente pelo pequeno teorema de Fermat, temos $8^{w^l} \equiv 8 \pmod{w}$ e, daí,

$$0 \equiv 8^q + 1 = 8^{w^l v} + 1 \equiv 8^v + 1 \pmod{w}, \tag{7.2}$$

de modo que $8^{2v} \equiv 1 \pmod{w}$. Sendo $t = \text{ord}_w(8)$, segue que $t \mid 2v$ e (pelo pequeno teorema de Fermat) $t \mid (w-1)$. Mas, como os fatores primos de v (se existirem) são maiores do que w, chegamos a $t = 1$ ou 2, de modo que $w \mid (8^1 - 1)$ ou $w \mid (8^2 - 1)$. Em qualquer caso, segue de $w > p = 3$ que $w = 7$ e, daí, (7.2) fornece

$$0 \equiv 8^v + 1 \equiv 1^v + 1 \equiv 2 \pmod{7},$$

um absurdo. Portanto, $q = 1$ e $n = 3^k q = 3$. ■

Problemas – Seção 7.2

1. Mostre que 2 é raiz primitiva módulo 29.

2. Se $m, n \in \mathbb{N}$ são tais que $m \mid n$, e $a \in \mathbb{Z}$ é uma raiz primitiva módulo n, prove que a também é raiz primitiva módulo m.

3. Prove a seguinte generalização do teorema de Wilson: se n é um natural que possui raízes primitivas e $1 = a_1 < a_2 < \cdots < a_{\varphi(n)} = n - 1$ são os inteiros de 1 a n e primos com n, então

$$n \mid (a_1 a_2 \ldots a_{\varphi(n)} + 1)$$

4. (Romênia.) Encontre todos os primos p e q distintos de 2 e de 3 e tais que $3pq \mid (a^{3pq-1} - 1)$, para todo natural a primo com $3pq$.

5. (OBM - adaptado.) Sejam $p > 5$ um primo tal que $\frac{p-1}{2}$ também é primo, e $f : \mathbb{Z}_+ \to \mathbb{R}$ uma função tal que $f(xy) = f(x)f(y)$ e $f(x+p) = f(x)$, para todos $x, y \in \mathbb{Z}_+$.

   (a) Mostre que $f(0), f(1) \in \{0, 1\}$ e que f é constante caso $f(0) = 1$ ou $f(1) = 0$.

   (b) Suponha, doravante, que $f(0) = 0$ e $f(1) = 1$. Use o pequeno teorema de Fermat para concluir que $f(a) \in \{-1, 1\}$, para todo $a \in \mathbb{N}$ tal que $p \nmid a$.

   (c) Se existe uma raiz primitiva a módulo p tal que $f(a) = 1$, então

$$f(x) = \begin{cases} 0, & \text{se } p \mid x \\ 1, & \text{se } p \nmid x \end{cases}.$$

   (d) Se $f(a) = -1$ para toda raiz primitiva a módulo p, então

$$f(x) = \begin{cases} 0, & \text{se } p \mid x \\ x^{p-1} \cdot (-1)^{\text{ord}_p(x)+1} \pmod{p}, & \text{se } p \nmid x \end{cases}.$$

6. (Turquia.) Prove que as duas afirmativas a seguir sobre $n \in \mathbb{N}$ são equivalentes:

   (a) n é livre de quadrados e, se p é um divisor primo de n, então $(p-1) \mid (n-1)$.

   (b) Para todo $a \in \mathbb{N}$, temos que $n \mid (a^n - a)$.

7. (Índia - adaptado.) Para $n \in \mathbb{N}$, seja $s_n = 1 + \sum_{k=1}^{n} k^{n-1}$. O propósito deste problema é caracterizar todos os $n \in \mathbb{N}$ tais que $n \mid s_n$. Para tanto, faça os seguintes itens:

   (a) Se p é primo e $q \in \mathbb{N}$, mostre que $p \mid \sum_{j=0}^{pq-1} \sum_{l=0}^{p-1} (pj+l)^{n-1}$.

   (b) Conclua que, se $n \mid s_n$, então n é livre de quadrados.

   (c) Seja $n = p_1 \ldots p_t$, com $p_1 < \cdots < p_t$ números primos, e $q_i = \frac{n}{p_i}$.

      i. Mostre que $s_n \equiv 1 + q_i \sum_{l=1}^{p_i - 1} l^{n-1} \pmod{p_i}$.

ii. Se a é uma raiz primitiva módulo p_i, mostre que

$$s_n \equiv 1 + q_i \left(\frac{a^{p_i(n-1)} - a^{n-1}}{a^{n-1} - 1} \right) \pmod{p_i}.$$

iii. A partir de ii., conclua sucessivamente que, se $n \mid s_n$, então $p_i \mid (a^{n-1}-1)$, $(p_i-1) \mid (n-1)$ e $(p_i-1) \mid (q_i-1)$.

iv. Se $n \mid s_n$, use os resultados dos itens i. e iii. para concluir que $p_i \mid (q_i - 1)$.

v. Prove, a partir dos dois itens anteriores, que $n \mid s_n$ se, e só se, $p_i(p_i - 1) \mid (q_i - 1)$ para $1 \leq i \leq t$.

8. Sejam p um primo ímpar, $k \neq p, 2p$ um natural tal que $1 \leq k < 2(p+1)$ e $n = 2pk + 1$.

(a) Se n é primo e a é uma raiz primitiva módulo n, prove que $\text{mdc}\,(a^k + 1, n) = 1$.

(b) Suponha que existe $2 \leq a < n$ inteiro, tal que $a^{kp} \equiv -1 \pmod{n}$ e $\text{mdc}\,(a^k + 1, n) = 1$.

i. Se $d = \text{ord}_n(a)$, mostre que $d \mid (n-1)$ e $d \nmid 2k$. Conclua que $p \mid d$ e, daí, que $p \mid \varphi(2kp+1)$.

ii. Use a fórmula para $\varphi(2kp+1)$ para concluir que existe $l > 1$ inteiro tal que $lp + 1$ é um divisor primo de n.

iii. Use que $n = 2kp+1$ para mostrar que $n = (lp+1)(hp+1)$ para algum inteiro $h \in \{0, 1\}$. Conclua, em seguida, que não podemos ter $h = 1$ e, daí, que n é primo.

O próximo problema é devido ao matemático francês do século XX Claude Chevalley, sendo conhecido como o **teorema de Chevalley**.

9. Se p é um primo ímpar, queremos mostrar que, módulo p, a congruência

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 \equiv 0 \pmod{p}$$

tem número de soluções igual a um múltiplo de p, onde duas soluções $(a_1, \ldots, a_5)$ e $(b_1, \ldots, b_5)$ são consideradas distintas se existir $1 \leq i \leq 5$ tal que $a_i \not\equiv b_i \pmod{p}$. Para tanto, faça os seguintes itens:

(a) Se $f(x_1, \ldots, x_5) = 1 - (x_1^4 + x_2^4 + \cdots + x_5^4)^{p-1}$ e m é o número de soluções da congruência do enunciado, então

$$m \equiv \sum_{x_1, \ldots, x_5 \in A} f(x_1, \ldots, x_5) \pmod{p},$$

onde $A = \{1, 2, \ldots, p-1\}$.

(b) Módulo p, temos

$$\begin{aligned} m &\equiv p^5 - \sum_{\alpha_1 + \cdots + \alpha_5 = p-1} \sum_{x_1, \ldots, x_5 \in A} x_1^{4\alpha_1} \ldots x_5^{4\alpha_5} \\ &\equiv - \sum_{\alpha_1 + \cdots + \alpha_5 = p-1} \left(\sum_{x_1 \in A} x_1^{4\alpha_1} \right) \ldots \left(\sum_{x_5 \in A} x_5^{4\alpha_5} \right). \end{aligned}$$

(c) Se $\alpha_1 + \cdots + \alpha_5 = p - 1$, com $\alpha_i \geq 0$ para $1 \leq i \leq 5$, então existe $1 \leq i \leq 5$ tal que $\alpha_i = 0$ ou $(p-1) \nmid 4\alpha_i$.

(d) Se $(p-1) \nmid 4\alpha$, use uma raiz primitiva a módulo p para concluir que

$$\sum_{x \in A} x^{4\alpha} = \sum_{j=1}^{p-1} a^{4j\alpha} = \frac{a^{4p\alpha} - a^{4\alpha}}{a^{4\alpha} - 1} \equiv 0 \pmod{p}.$$

(e) Conclua que $m \equiv 0 \pmod{p}$.

7.3 Resíduos quadráticos

Estudamos, nesta seção, congruências algébricas da forma

$$x^2 \equiv a \pmod{n}.$$

Precisamos, inicialmente, da definição a seguir.

Definição 7.17. Se $a, n \in \mathbb{Z}$, com $n > 1$ e $\text{mdc}\,(a, n) = 1$, diremos que a é um **resíduo quadrático** módulo n se a congruência

$$x^2 \equiv a \pmod{n}$$

possuir pelo menos uma solução inteira x. Caso contrário, a é dito um **não resíduo quadrático** módulo n.

Em relação à definição acima, nossa tarefa primordial será obter condições necessárias e suficientes para que um inteiro a seja resíduo quadrático módulo n. Analisemos o caso em que n é primo, deixando o caso geral para os problemas propostos ao final desta seção.

Proposição 7.18. Seja p um primo ímpar.

(a) Se a é um resíduo quadrático módulo p, então a congruência $x^2 \equiv a \pmod{p}$ possui exatamente duas soluções incongruentes módulo p.

(b) Dentre os números $1, 2, \ldots, p-1$ há exatamente $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ não resíduos quadráticos módulo p.

Prova.
(a) Se x_1 e x_2 são inteiros tais que $x_1^2 \equiv a \pmod{p}$ e $x_2^2 \equiv a \pmod{p}$, então $x_1^2 \equiv x_2^2 \pmod{p}$, de sorte que $p \mid (x_1^2 - x_2^2)$. Mas, como p é primo, segue que $p \mid (x_1 - x_2)$ ou $p \mid (x_1 + x_2)$. Portanto, a congruência do enunciado possui no máximo duas raízes incongruentes, quais sejam, x_1 e $p - x_1$. Por outro lado, sendo a um resíduo quadrático módulo p, sabemos que tal congruência admite uma solução $x_0 \in \mathbb{Z}$. Segue imediatamente que $p - x_0$ também é solução da referida congruência, com $p - x_0 \not\equiv x_0 \pmod{p}$, uma vez que p é ímpar e $\text{mdc}\,(x_0, p) \mid \text{mdc}\,(a, p) = 1$.

(b) Como $\{1, 2, \ldots, p-1\}$ é um SCI módulo p, para contarmos quantos de seus elementos são resíduos quadráticos, módulo p, basta calcularmos quantos dentre os números $1^2, 2^2, \ldots, (p-1)^2$ são dois a dois incongruentes, módulo p. Para tanto, veja que, se $1 \leq i \leq \frac{p-1}{2}$, então

$$i^2 \equiv (p-i)^2 \pmod{p};$$

por outro lado, se $1 \leq i < j \leq \frac{p-1}{2}$, então

$$i^2 \not\equiv j^2 \pmod{p},$$

uma vez que $j^2 - i^2 = (j-i)(j+i)$ e $0 < j - i < j + i < p$.

Logo, há precisamente $\frac{p-1}{2}$ resíduos quadráticos módulo p e, daí, $(p-1) - \left(\frac{p-1}{2}\right) = \frac{p-1}{2}$ não resíduos quadráticos módulo p. ■

O resultado a seguir é devido a L. Euler, sendo conhecido na literatura como o **critério de Euler** para resíduos quadráticos.

Proposição 7.19 (Euler)**.** Se p é um primo ímpar, então um inteiro a é resíduo quadrático módulo p se, e só se,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Prova. Suponha primeiro que a é resíduo quadrático módulo p. Então, $\text{mdc}\,(a, p) = 1$ e existe $x_0 \in \mathbb{Z}$ tal que $x_0^2 \equiv a \pmod{p}$. Em particular, x_0 também é primo com p, e o pequeno teorema de Fermat fornece

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1 \pmod{p}.$$

Reciprocamente, suponha que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, de sorte que, em particular, $\text{mdc}\,(a, p) = 1$. Então, sendo α uma raiz primitiva módulo p, temos que $\{\alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ é um SCI módulo p e, daí, existe um inteiro $1 \leq k \leq p-1$ tal que $\alpha^k \equiv a \pmod{p}$. Portanto,

$$\alpha^{k\left(\frac{p-1}{2}\right)} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

e segue de $\text{ord}_p(\alpha) = p - 1$ que $(p-1) \mid k\left(\frac{p-1}{2}\right)$, de maneira que k é par, digamos $k = 2l$. Fazendo $x_0 = \alpha^l$, temos

$$x_0^2 = \alpha^{2l} = \alpha^k \equiv a \pmod{p},$$

de sorte que a é um resíduo quadrático módulo p. ■

Corolário 7.20. Se p é um primo ímpar, então um inteiro a primo com p é um não resíduo quadrático módulo p se e só se

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Prova. Pelo pequeno teorema de Fermat, temos

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Mas, como p é primo, temos que

$$a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \text{ ou } a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}.$$

Por outro lado, pelo critério de Euler, a é um não resíduo quadrático módulo p se, e só se, a primeira das duas congruências acima não ocorre, i.e., se, e só se, $a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$. ■

Observação 7.21. É possível provar (cf. problema 8.2.7 do volume 6) que, para todo $a \in \mathbb{Z}$, existem infinitos primos p tais que a não é resíduo quadrático módulo p.

A fim de facilitar as manipulações com resíduos e não resíduos quadráticos, precisamos de uma notação conveniente, a qual é introduzida pela definição a seguir.

Definição 7.22. Dados inteiros a e p, com p primo, definimos o **símbolo de Legendre** $\left(\frac{a}{p}\right)$ por:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ for resíduo quadrático modulo } p \\ -1, & \text{se } a \text{ for não resíduo quadrático modulo } p \\ 0, & \text{se } p \mid a \end{cases}.$$

A conveniência notacional do símbolo de Legendre é esclarecida pelas duas próximas proposições.

Proposição 7.23. Se p é um primo ímpar e $a, b \in \mathbb{Z}$, então:

(a) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(b) Se $p \nmid a$, então $\left(\frac{a^2}{p}\right) = 1$.

(c) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(d) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Prova. A prova dos itens (a) e (b) é imediata. Provemos, pois, o item (c): se $p \mid a$, então

$$\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}} \pmod{p};$$

senão, a proposição 7.19 e o corolário 7.20 garantem que, modulo p,

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \text{ se } a \text{ for resíduo quadrático módulo } p \\ -1 \text{ se } a \text{ for não resíduo quadrático módulo } p \end{cases} = \left(\frac{a}{p}\right).$$

Por fim, quanto a (d), observe que, se $p \mid ab$, então $p \mid a$ ou $p \mid b$ e, daí,

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 0 = \left(\frac{ab}{p}\right).$$

Por outro lado, se $p \nmid ab$, então $p \nmid a$ e $p \nmid b$, e segue do item (c) que

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

Portanto, p divide a diferença $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right)$, a qual assume um dos valores inteiros de -2 a 2. Mas, como p é ímpar, concluímos que deve ser $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) - \left(\frac{ab}{p}\right) = 0$. ■

O exemplo a seguir mostra como utilizar as propriedades do símbolo de Legendre deduzidas na proposição acima.

Exemplo 7.24. Prove que não existem x e y inteiros tais que $y^2 = x^3 + 7$.

Solução. Suponha o contrário. Então x é ímpar, pois, do contrário, teríamos $y^2 = x^3 + 7 \equiv 3 (\bmod 4)$, uma contradição ao item (c) da proposição 5.9.

Por outro lado,

$$y^2 + 1 = x^3 + 8 = (x+2)[(x-1)^2 + 3] \tag{7.3}$$

e, como $(x-1)^2 + 3 \equiv 3 (\bmod 4)$ (lembre-se de que $x - 1$ é par), existe um primo p da forma $4k + 3$ tal que p divide $(x-1)^2 + 3$.

Voltando a (7.3), concluímos que $y^2 + 1 \equiv 0 \,(\bmod p)$, i.e., que -1 é resíduo quadrático módulo p. Segue da definição do símbolo de Legendre e do item (c) da proposição anterior que, módulo p,

$$1 = \left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1,$$

uma contradição. ■

Nosso próximo resultado, devido a K. F. Gauss e conhecido na literatura como o **lema de Gauss**, fornece um procedimento bem mais simples que o critério de Euler para decidir se um certo inteiro é resíduo ou não resíduo quadrático módulo p, sendo p um primo ímpar dado.

Proposição 7.25 (Gauss)**.** Se p é um primo ímpar e a é primo com p, então $\left(\frac{a}{p}\right) = (-1)^m$, onde m é o número de elementos do conjunto

$$\left\{1 \le j \le \frac{p-1}{2};\ ja \equiv -1, -2, \ldots \text{ ou } -\left(\frac{p-1}{2}\right) (\bmod p)\right\}. \tag{7.4}$$

Prova. Para $1 \le j \le \frac{p-1}{2}$, seja $-\frac{p-1}{2} \le t_j \le \frac{p-1}{2}$ o inteiro tal que

$$ja \equiv t_j \,(\bmod p).$$

Provemos primeiro que

$$1 \le i < j \le \frac{p-1}{2} \Rightarrow |t_i| \ne |t_j|.$$

Para tanto, basta ver que, como $\text{mdc}\,(a,p) = 1$, temos

$$\begin{aligned} |t_i| = |t_j| \quad &\Rightarrow \quad |ia| \equiv |ja| \,(\bmod p) \Rightarrow |i| \equiv |j| \,(\bmod p) \\ &\Rightarrow \quad i \pm j \equiv 0 \,(\bmod p), \end{aligned}$$

o que é impossível.

Segue do que fizemos acima que os números $|t_1|, \ldots, |t_{\frac{p-1}{2}}|$ formam, em alguma ordem, uma permutação dos números $1, 2, \ldots, \frac{p-1}{2}$ (veja que nenhum deles é igual a 0, já que $\text{mdc}\,(a,p) = 1$). Portanto, lembrando que m denota a quantidade de índices j para os quais $t_j < 0$, temos, módulo p, que

$$(-1)^m a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^m t_1 \ldots t_{\frac{p-1}{2}} = |t_1| \ldots |t_{\frac{p-1}{2}}| = \left(\frac{p-1}{2}\right)!$$

e, daí,

$$a^{\frac{p-1}{2}} \equiv (-1)^m \,(\bmod p).$$

O resto segue do item (c) da proposição 7.23. ■

Como aplicação do lema de Gauss, mostramos a seguir que 2 é resíduo quadrático módulo p se, e só se, $p \equiv 0, 1, 2$ ou $7 \,(\bmod 8)$.

Exemplo 7.26. Se p é um primo ímpar, então

$$\left(\frac{2}{p}\right) = (-1)^{\lfloor \frac{p+1}{4} \rfloor} = (-1)^{\frac{p^2-1}{8}}.$$

Prova. Pelo lema de Gauss, temos $\left(\frac{2}{p}\right) = (-1)^m$, onde

$$m = \#\left\{1 \leq k \leq \frac{p-1}{2};\ 2k \equiv -1, -2, \ldots \text{ ou } -\left(\frac{p-1}{2}\right) \pmod p\right\}.$$

Se $1 \leq k \leq \lfloor \frac{p-1}{4} \rfloor$, então $2 \leq 2k \leq 2\lfloor \frac{p-1}{4} \rfloor \leq \frac{p-1}{2}$ e, daí,

$$2k \not\equiv -1, -2, \ldots, -\left(\frac{p-1}{2}\right) \pmod p.$$

Se $\lfloor \frac{p-1}{4} \rfloor + 1 \leq k \leq \frac{p-1}{2}$, então

$$p - 1 \geq 2k \geq 2\left(\left\lfloor \frac{p-1}{4} \right\rfloor + 1\right) > 2\left(\frac{p-1}{4} - 1\right) + 2 = \frac{p-1}{2};$$

em particular, $2k \not\equiv 1, 2, \ldots, \frac{p-1}{2} \pmod p$, ou, o que é o mesmo,

$$2k \equiv -1, -2, \ldots \text{ ou } -\left(\frac{p-1}{2}\right) \pmod p.$$

Portanto,

$$m = \frac{p-1}{2} - \left(\left\lfloor \frac{p-1}{4} \right\rfloor + 1\right) + 1 = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = \left\lfloor \frac{p+1}{4} \right\rfloor,$$

onde, para a última igualdade, basta considerarmos separadamente os casos $p = 4k + 1$ e $p = 4k + 3$.

Quanto à segunda igualdade, é suficiente mostrarmos que

$$\left\lfloor \frac{p+1}{4} \right\rfloor \equiv \frac{p^2 - 1}{8} \pmod 2.$$

Para tanto, basta considerarmos separadamente os casos $p = 8k + 1$, $p = 8k + 3$, $p = 8k + 5$ e $p = 8k + 7$. ■

Prosseguindo em nosso estudo de resíduos quadráticos, vamos provar um dos mais famosos teoremas de Gauss, o qual estabelece uma relação simples entre os símbolos de Legendre $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$, onde p e q são primos ímpares. Comecemos reformulando o lema de Gauss.

Lema 7.27. Se p é um primo ímpar e a é um inteiro primo com p e também ímpar, então $\left(\frac{a}{p}\right) = (-1)^M$, onde

$$M = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor.$$

Prova. Para $1 \leq j \leq \frac{p-1}{2}$, seja $0 < r_j < p$ o resto da divisão de ja por p, de maneira que (cf. proposição 1.7)

$$ja = \left\lfloor \frac{ja}{p} \right\rfloor p + r_j. \tag{7.5}$$

É imediato que

$$ja \equiv -1, -2, \ldots, -\left(\frac{p-1}{2}\right) \pmod p \Leftrightarrow \frac{p+1}{2} \leq r_j < p.$$

Portanto, nas notações do lema de Gauss, há exatamente m índices $1 \leq j \leq \frac{p-1}{2}$ tais que $\frac{p+1}{2} \leq r_j < p$, e basta mostrarmos que a paridade do número de tais índices é, por outro lado, igual à de $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$.

Para o que falta, denote por $s_1, s_2, \ldots, s_m$ (após uma reenumeração, se necessário) os restos r_j tais que $\frac{p+1}{2} \leq r_j < p$, e por $t_1, \ldots, t_n$ (também após uma reenumeração, se necessário) os restos r_j tais que $1 \leq r_j \leq \frac{p-1}{2}$. Então $m + n = \frac{p-1}{2}$ e (assim como na prova do lema de Gauss), para $1 \leq i < j \leq \frac{p-1}{2}$ temos $r_i \neq r_j, p - r_j$. Logo,

$$\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{p - s_1, p - s_2, \ldots, p - s_m\} \cup \{t_1, t_2, \ldots, t_n\},$$

uma união disjunta, e, daí,

$$\frac{p^2 - 1}{8} = \sum_{j=1}^{\frac{p-1}{2}} j = mp - \sum_{j=1}^{m} s_j + \sum_{j=1}^{n} t_j.$$

Por outro lado, somando as igualdades (7.5) sobre $1 \leq j \leq \frac{p-1}{2}$, obtemos

$$a\left(\frac{p^2-1}{8}\right) = p\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor + \sum_{j=1}^{m} s_j + \sum_{j=1}^{n} t_j.$$

Subtraindo membro a membro as duas relações acima, segue então que

$$(a-1)\left(\frac{p^2-1}{8}\right) = p\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor - mp + 2\sum_{j=1}^{m} s_j;$$

por fim, lembrando que a e p são ímpares e analisando a igualdade acima módulo 2, obtemos

$$0 \equiv \sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{ja}{p}\right\rfloor - m,$$

conforme desejado. ■

O teorema a seguir é conhecido na literatura como a **lei da reciprocidade quadrática** de Gauss, e a prova que apresentamos é devido ao matemático alemão do século XIX Ferdinand Eisenstein.

Teorema 7.28 (Gauss). Se p e q são primos ímpares e distintos, então

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

Prova. Pelo lema anterior, temos

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^m(-1)^n,$$

onde

$$m = \sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor \quad \text{e} \quad n = \sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{jq}{p}\right\rfloor.$$

É, então, suficiente mostrarmos que

$$\sum_{j=1}^{\frac{p-1}{2}}\left\lfloor\frac{jq}{p}\right\rfloor + \sum_{j=1}^{\frac{q-1}{2}}\left\lfloor\frac{jp}{q}\right\rfloor = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right), \tag{7.6}$$

para o quê utilizamos o seguinte argumento geométrico: como o segundo membro da igualdade acima é igual ao número de pontos de coordenadas inteiras no retângulo fechado

$$\mathcal{R} = \left\{(x,y) \in \mathbb{R}^2;\ 1 \leq x \leq \frac{p-1}{2} \text{ e } 1 \leq y \leq \frac{q-1}{2}\right\},$$

basta contarmos o número de tais pontos de outra maneira, obtendo o primeiro membro de (7.6) como resultado.

Sem perda de generalidade, suponha que $p > q$, e considere a reta $y = \frac{q}{p}x$ (cf. figura 7.1). Para cada $j \geq 1$, o número $\left\lfloor\frac{jq}{p}\right\rfloor$ conta o

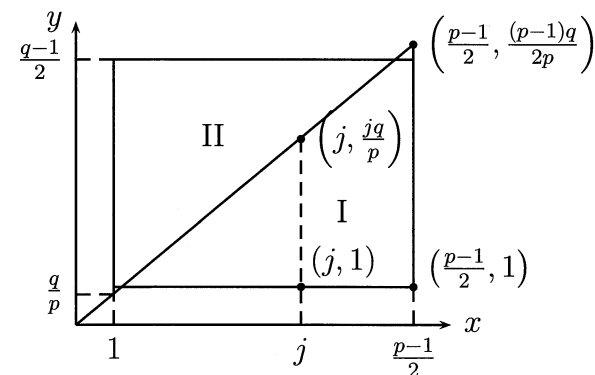



Figura 7.1: contando os pontos de $\mathcal{R} \cap \mathbb{Z}^2$.

número de inteiros positivos menores ou iguais que $\frac{jq}{p}$; por outro lado, para $1 \leq j \leq \frac{p-1}{2}$ temos que $\frac{jq}{p} \notin \mathbb{Z}$ e, daí, $\left\lfloor\frac{jq}{p}\right\rfloor$ conta o número de pontos de coordenadas inteiras situados sobre a reta $x = j$, abaixo da

reta $y = \frac{q}{p}x$ e acima da reta $y = 0$. Mas, como

$$\left\lfloor \frac{jq}{p} \right\rfloor \leq \left\lfloor \frac{(p-1)q}{2p} \right\rfloor = \left\lfloor \frac{q}{2} - \frac{q}{2p} \right\rfloor \leq \left\lfloor \frac{q}{2} \right\rfloor = \frac{q-1}{2},$$

todos os pontos que estamos contando de fato pertencem ao retângulo $\mathcal{R}$. Portanto, nas notações da figura 7.1, temos

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor = \# \text{ de pontos de coordenadas inteiras na região I de } \mathcal{R}.$$

Analogamente,

$$\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor = \# \text{ de pontos de coordenadas inteiras na região II de } \mathcal{R}$$

e nada mais há a fazer. ■

Terminamos esta seção com uma aplicação da lei da reciprocidade quadrática à existência de certos tipos de números primos.

Exemplo 7.29. Prove que há infinitos primos da forma $3k+1$, $k \in \mathbb{N}$.

Prova. Por absurdo, suponhamos que houvesse somente uma quantidade finita de primos da forma $3k+1$, digamos $p_1, p_2, \ldots, p_n$, e seja $x = (2p_1 \ldots p_n)^2 + 3$. Sendo p um divisor primo de x, é claro que $p \neq 2, 3, p_1, \ldots, p_n$, de modo que $p \equiv -1 \pmod 3$. Ademais, como

$$(2p_1 \ldots p_n)^2 \equiv -3 \pmod p,$$

temos que -3 é resíduo quadrático módulo p. Devemos, então, ter $\left(\frac{-3}{p}\right) = 1$. Mas

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right), \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

e, pela lei da reciprocidade quadrática,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{3-1}{2}\right)} = (-1)^{\frac{p-1}{2}}.$$

Assim,

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)^{-1}(-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right).$$

Por fim, $p \equiv -1 \pmod 3$ implica, pelo item (a) da proposição 7.23, que $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1$; por sua vez, tal igualdade contradiz o fato de -3 ser um resíduo quadrático módulo p. ■

Problemas – Seção 7.3

1. Se p é um primo ímpar, prove que -1 é resíduo quadrático módulo p se, e só se, $p \equiv 1 \pmod 4$.
2. Prove que a equação $x^2 = y^3 + k$ não admite soluções inteiras x, y para infinitos valores inteiros de k.
3. Sejam a, b e c inteiros não todos nulos e n um natural. Se existem inteiros x e y, relativamente primos com n e tais que $ax^2 + bxy + cy^2 = n$, prove que $b^2 - 4ac$ é um resíduo quadrático módulo n.
4. Prove que não existem $x, y \in \mathbb{Z}$ tais que $x^2 + 3xy - 2y^2 = 122$.
5. Dados $a, b \in \mathbb{Z}$, mostre que:

   (a) $2b^2 + 3$ tem um divisor primo p, tal que $p \equiv \pm 3 \pmod 8$.

   (b) $(2b^2 + 3) \nmid (a^2 - 2)$.

6. Se $p \neq 3$ é um primo ímpar, prove que

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{se } p \equiv \pm 1 \pmod{12} \\ -1, & \text{se } p \equiv \pm 5 \pmod{12} \end{cases}.$$

7. Sejam m e n naturais ímpares, com $n > 1$.

   (a) $2^n - 1$ tem um divisor primo p, tal que $p \equiv \pm 5 \pmod{12}$.

   (b) $(2^n - 1) \nmid (3^m - 1)$.

8. Se $n > 1$ é um natural tal que $p = 2^n + 1$ é primo, faça os seguintes itens:

   (a) Mostre que 3 é um não resíduo quadrático, módulo p.

   (b) Conclua que 3 é raiz primitiva, módulo p.

9. (a) Sejam a e k inteiros dados, sendo a ímpar. Prove que a congruência $x^2 \equiv a \pmod{2^k}$ tem solução para todo $k > 2$ se, e só se, a congruência $x^2 \equiv a \pmod 8$ tem solução.

   (b) Sejam p um primo ímpar e a um inteiro primo com p. Prove que a congruência $x^2 \equiv a \pmod{p^k}$ tem solução para todo $k \geq 1$ se, e só se, a congruência $x^2 \equiv a \pmod p$ tem solução.

10. * Sejam a e n naturais primos entre si, com $n > 1$, e $n = 2^k p_1^{k_1} \dots p_t^{k_t}$ a decomposição canônica de n em fatores primos. Prove que a congruência $x^2 \equiv a \pmod n$ tem solução se, e só se, forem satisfeitas as seguintes condições:

    (i) $a \equiv 1 \pmod 2$ se $k = 1$, $a \equiv 1 \pmod 4$ se $k = 2$ ou $a \equiv 1 \pmod 8$ se $k \geq 3$.

    (ii) $a^{\frac{p_i - 1}{2}} \equiv 1 \pmod{p_i}$, para $1 \leq i \leq t$.

11. (APMO.) Durante um recreio, o professor reuniu seus n alunos no pátio da escola, formando com os mesmos um círculo. Em seguida, escolheu um aluno, deu a ele um doce e, no sentido anti-horário, saiu distribuindo doces aos alunos da seguinte maneira: pulou um aluno e entregou um doce ao terceiro, pulou dois alunos e entregou um doce ao sexto aluno, pulou três alunos e entregou um doce ao décimo e assim por diante, sempre pulando um aluno a mais que na vez anterior e entregando um doce ao próximo. Para que valores de n cada aluno terá recebido ao menos um doce após um número finito e suficientemente grande de voltas?

12. Dados um primo p e inteiros primos entre si a e n, com $n > 1$, dizemos que a é um **resíduo n−ésimo**, módulo p, se a congruência $x^n \equiv a \pmod p$ tiver solução. Generalize o critério de Euler para resíduos quadráticos, do seguinte modo: se $d = \text{mdc}\,(n, p-1)$, então

$$a \text{ é um resíduo } n - \text{ésimo módulo } p \Leftrightarrow a^{\frac{p-1}{d}} \equiv 1 \pmod p.$$

Para o próximo problema, o leitor necessitará utilizar alguns fatos básicos sobre as *somas simétricas elementares* das raízes de um polinômio, para o quê sugerimos a leitura da seção 4.2 do volume 6.

13. (Bulgária - adaptado.) O objetivo deste problema é mostrar que, se $p > 5$ é primo e $k > 1$ é inteiro, então $p^3 \mid \left(\binom{kp}{p} - k\right)$. Para tanto, faça os seguintes itens:

    (a) Suponha, até o item (f), que k é ímpar. Conclua que

$$\binom{kp}{p} - k = \frac{k}{(p-1)!}(f(\alpha) - f(-\alpha)),$$

    onde $f(x) = \prod_{j=1}^{p-1}\left(x + \frac{(k-1)p}{2} + j\right)$, um polinômio de coeficientes inteiros, e $\alpha = \frac{(k-1)p}{2}$.

(b) Se $f(x) = x^{p-1} + a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_1x + a_0$, mostre que $f(\alpha) - f(-\alpha) \equiv 2a_1\alpha \pmod{p^3}$ e deduza, a partir daí, que basta mostrar que $a_1 \equiv 0 \pmod{p^2}$.

(c) Use as relações de Girard (cf. proposição 4.6 do volume 6) para mostrar que a condição $a_1 \equiv 0 \pmod{p^2}$ equivale à congruência $\sum_{j=1}^{\frac{p-1}{2}} r_j \equiv 0 \pmod{p}$, onde $r_j = \prod_{\substack{1 \leq i \leq \frac{p-1}{2} \\ i \neq j, p-j}} (\alpha + i)$.

(d) Mostre que a igualdade $(\alpha + j)(\alpha + p - j)r_j = \prod_{i=1}^{\frac{p-1}{2}} (\alpha + i)$ implica, módulo p, a congruência $j^2 r_j \equiv -(p-1)! \pmod{p}$, para $1 \leq j \leq \frac{p-1}{2}$.

(e) Conclua, a partir do item (d), que r_j é um resíduo quadrático, módulo p e $r_i \not\equiv r_j \pmod{p}$, para todos $1 \leq i < j \leq \frac{p-1}{2}$.

(f) Deduza que, módulo p, o conjunto $\{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\}$ forma uma permutação do conjunto $\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$ e conclua o que se pede.

(g) Se k for par, siga os passos delineados nos itens de (a) a (f), argumentando, de início, com o polinômio $f(x) = \prod_{j=1}^{p-1} \left(x + \frac{kp}{2} - j\right)$.

7.4 Somas de quadrados

Como aplicação das ideias desenvolvidas até aqui, caracterizaremos nesta seção os naturais que podem ser escritos como soma de dois quadrados. Comecemos pelo caso dos números primos, com o seguinte resultado de Fermat.

Teorema 7.30 (Fermat). As seguintes condições sobre um primo ímpar p são equivalentes:

(a) $p \equiv 1 \pmod{4}$.

(b) -1 é resíduo quadrático módulo p.

(c) p pode ser escrito como soma de dois quadrados.

Prova.
(a) $\Rightarrow$ (b): sendo $p = 4k + 1$, segue do item (c) da proposição 7.23 que

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2k} \equiv 1 \pmod{p}$$

e, daí, -1 é resíduo quadrático módulo p.

(b) $\Rightarrow$ (c): sejam $h \in \mathbb{Z}$ tal que $h^2 + 1 \equiv 0 \pmod{p}$, e

$$A = \{(x, y);\ x, y \in \mathbb{Z},\ 0 \leq x, y < \sqrt{p}\}.$$

Pelo princípio fundamental da contagem (cf. corolário 1.9 do volume 4), temos $|A| = \left(\lfloor\sqrt{p}\rfloor + 1\right)^2$. Agora, como

$$(\lfloor\sqrt{p}\rfloor + 1)^2 > \sqrt{p}^2 = p$$

e só há p possíveis restos numa divisão por p, o princípio da casa dos pombos (cf. seção 4.1 do volume 4) garante a existência de pares ordenados distintos $(x_1, y_1), (x_2, y_2) \in A$, tais que

$$hx_1 + y_1 \equiv hx_2 + y_2 \pmod{p}.$$

Fazendo $a = |x_1 - x_2|$ e $b = |y_1 - y_2|$, temos a e b não ambos nulos e, daí,

$$0 < a^2 + b^2 = |x_1 - x_2|^2 + |y_1 - y_2|^2 < \sqrt{p}^2 + \sqrt{p}^2 = 2p.$$

Mas, como

$$\begin{aligned} a^2 + b^2 &= |x_1 - x_2|^2 + |y_1 - y_2|^2 \equiv (x_1 - x_2)^2 + (hx_1 - hx_2)^2 \\ &= (h^2 + 1)(x_1 - x_2)^2 \equiv 0 \pmod{p}, \end{aligned}$$

a única possibilidade é que seja $a^2 + b^2 = p$.

(c) $\Rightarrow$ (a): se $p = a^2 + b^2$, com $a, b \in \mathbb{Z}$, então a é par e b é ímpar ou vice-versa (lembre-se de que p é ímpar). Supondo, sem perda de generalidade, que a é par e b é ímpar, segue da proposição 5.9 que

$$p = a^2 + b^2 \equiv 0 + 1 \equiv 1 \pmod 4.$$

■

Para prosseguir, precisamos de um resultado auxiliar, usualmente atribuído a Euler e conhecido como a **identidade de Euler**.

Lema 7.31. Se m e n são naturais que podem ser escritos como somas de dois quadrados, então mn também pode ser escrito como soma de dois quadrados.

Prova. Se $m = a^2 + b^2$ e $n = c^2 + d^2$, então

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) \\ &= ((ac)^2 + (bd)^2) + ((ad)^2 + (bc)^2) \qquad (7.7) \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

■

O teorema a seguir, também atribuído a Fermat, dá uma condição necessária e suficiente para um natural poder ser escrito como soma de dois quadrados.

Teorema 7.32 (Fermat)**.** Um natural n pode ser escrito como soma de dois quadrados se, e só se, $n = 1$ ou n é tal que todo primo congruente a 3 módulo 4 e que comparece na fatoração canônica de n o faz com expoente par.

Prova. No que segue, seja

$$n = 2^a p_1^{a_1} \ldots p_k^{a_k} q_1^{b_1} \ldots q_l^{b_l}$$

a decomposição de n em fatores primos, com $a, a_i, b_j \geq 0$, $p_i \equiv 1 \pmod 4$ e $q_j \equiv 3 \pmod 4$, para todos $1 \leq i \leq k$ e $1 \leq j \leq l$.

(i) Se cada b_j for par, então n pode ser escrito como soma de dois quadrados: note inicialmente que, pelo teorema 7.30, cada p_i pode ser escrito como soma de dois quadrados; por outro lado, temos $2^a = (2^{a/2})^2 + 0^2$ se a for par e $2^a = (2^{(a-1)/2})^2 + (2^{(a-1)/2})^2$ se a for ímpar; por fim, se $b_j = 2c_j$, com $c_j \in \mathbb{Z}$ para $1 \leq j \leq l$, então $q_j^{b_j} = (q_j^{c_j})^2 + 0^2$. Portanto, aplicando repetidamente o lema 7.31, concluímos que n pode ser escrito como soma de dois quadrados.

(ii) Se n puder ser escrito como soma de dois quadrados, então cada b_j é par: é suficiente provar que se n pode ser escrito como soma de dois quadrados e $b_j \geq 1$, então $b_j \geq 2$ e $\frac{n}{q_j^2}$ também pode ser escrito como soma de dois quadrados. Para tanto, se $n = c^2 + d^2$, com $c, d \in \mathbb{Z}$, então $c^2 + d^2 \equiv 0 \pmod{q_j}$. Se $d \not\equiv 0 \pmod{q_j}$, então $\mathrm{mdc}\,(d, q_j) = 1$, de sorte que d é invertível, módulo q_j; sendo f seu inverso, módulo q_j, obtemos

$$(cf)^2 + 1 \equiv 0 \pmod{q_j},$$

em contradição ao teorema 7.30, uma vez que $q_j \equiv 3 \pmod 4$. Portanto, $d \equiv 0 \pmod{q_j}$ e, daí, $c \equiv 0 \pmod{q_j}$. Logo, $n = c^2 + d^2 \equiv 0 \pmod{q_j^2}$, de forma que $b_j \geq 2$ e

$$\frac{n}{q_j^2} = \left(\frac{c}{q_j}\right)^2 + \left(\frac{d}{q_j}\right)^2.$$

■

Terminemos esta seção mostrando que a maneira de escrever um primo da forma $4k + 1$ como soma de dois quadrados é essencialmente única.

Proposição 7.33. Se p é um primo da forma $4k+1$, então existem únicos $x, y \in \mathbb{N}$ tais que $x < y$ e $x^2 + y^2 = p$.

Prova. Já sabemos que existe ao menos um par de naturais x, y tais que $x^2 + y^2 = p$. Seja, então, a, b um outro tal par e observe que a, b, x e y são todos primos com p e menores que $\sqrt{p}$. Escolha inteiros $1 \leq c, z < p$ tais que $xz \equiv y$ e $ac \equiv b \pmod{p}$.

Afirmamos que $c = z$ ou $c + z = p$. De fato, módulo p, temos

$$x^2 + y^2 \equiv x^2 + (xz)^2 = x^2(z^2 + 1),$$

de maneira que $z^2 \equiv -1 \pmod{p}$. Analogamente, $c^2 \equiv -1 \pmod{p}$, de modo que p divide $z^2 - c^2 = (z-c)(z+c)$ e, daí, p divide $z - c$ ou $z + c$. Mas, como $1 \leq c, z < p$, segue que $-p < z - c < z + c < 2p$, acarretando em $z - c = 0$ ou $z + c = p$.

Suponha, agora, que $c = z$. As escolhas de c e z garantem que

$$bxz \equiv acy \equiv ayz \pmod{p} \tag{7.8}$$

e, daí, $bx \equiv ay \pmod{p}$. Mas, uma vez que $0 < a, b, x, y < \sqrt{p}$, temos $0 < bx, ay < p$ e, por conseguinte, $bx = ay$. Assim,

$$p = x^2 + y^2 = \left(\frac{ay}{b}\right)^2 + y^2 = \left(\frac{y}{b}\right)^2 (a^2 + b^2) = \left(\frac{y}{b}\right)^2 p$$

e, daí, $y = b$ e $x = a$.

Se $z + c = p$, então, argumentando como em (7.8), chegamos a $bx \equiv -ay \pmod{p}$ e, daí, a $bx + ay = p$. Então, (7.7) fornece

$$p^2 = (a^2 + b^2)(x^2 + y^2) = (bx + ay)^2 + (by - ax)^2 = p^2 + (by - ax)^2,$$

ou seja, $by = ax$. Novamente como acima, concluímos que $x = b$ e $y = a$. ■

Problemas – Seção 7.4

1. O propósito deste problema é mostrar que nem todo natural pode ser escrito como soma de três quadrados. Para tanto, prove o seguinte teorema de Euler: não existem inteiros k, l, x, y, z tais que $l \geq 0$ e
$$x^2 + y^2 + z^2 = 4^l(8k + 7).$$

2. Se $a, b, c \in \mathbb{N}$ são tais que $a(a-1) = b^2 + c^2$, mostre que $a + b$ é ímpar.

3. (BMO.) Encontre todos os pares de naturais distintos x e y, tais que $\frac{x^2+y^2}{x-y}$ seja um inteiro divisor de 1995.

4. Dado n natural, prove que existem n naturais consecutivos, tais que nenhum deles pode ser escrito como soma de dois quadrados.

5. O propósito deste problema é provar um teorema, devido a Joseph L. Lagrange, que afirma que todo natural pode ser escrito como uma soma de quatro quadrados. Para tanto, observamos inicialmente que vale a seguinte generalização do lema 7.31: se dois naturais m e n podem ser escritos como somas de quatro quadrados, então mn também pode ser escrito como uma soma de quatro quadrados. De fato, se $m = a^2 + b^2 + c^2 + d^2$ e $n = w^2 + x^2 + y^2 + z^2$, o leitor pode verificar sem dificuldade que[1]
$$\begin{aligned} mn &= (aw - bx - cy - dz)^2 + (ax + bw + cz - dy)^2 \\ &\quad + (ay - bz + cw + dx)^2 + (az + by - cx + dw)^2. \end{aligned} \tag{7.9}$$
De posse de tal resultado, faça os seguintes itens:

[1]Para uma prova natural da identidade em questão, referimos o leitor ao problema 1.1.9 da segunda edição do volume 6.

(a) Sejam p primo, $S = \{x^2;\ x \in \mathbb{Z}_p\}$ e $S' = \{\overline{-1} - y;\ y \in S\}$. Prove que $S \cap S' \neq \emptyset$.

(b) Conclua que, se p é primo, então existem $x, y, m \in \mathbb{Z}$ tais que $1 \leq m < p$ e $x^2 + y^2 + 1 = mp$.

(c) Sejam p um primo e $1 < m < p$ tal que $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$, onde os x_i's são inteiros. Se $-\frac{m}{2} < y_i < \frac{m}{2}$ é tal que $x_i \equiv y_i \pmod{m}$, prove que existe $1 \leq r < m$ tal que $rp = y_1^2 + y_2^2 + y_3^2 + y_4^2$.

(d) Mostre que todo número natural pode ser escrito como uma soma de quatro quadrados.

6. O propósito deste problema é encontrar todos os $n \in \mathbb{N}$ para os quais existe $m \in \mathbb{N}$ tal que $2^n - 1$ divide $m^2 + 9$. Para tanto, faça os dois itens a seguir:

   (a) Mostre, por contradição, que, se $2^n - 1$ divide $m^2 + 9$ para algum $m \in \mathbb{N}$, então n é uma potência de 2.

   (b) Se $n = 2^k$ mostre, por indução sobre k, que existe $m_k \in \mathbb{N}$ tal que $2^{2^k} - 1$ divide $m_k^2 + 9$.

CAPÍTULO 8

Sugestões e Soluções

Seção 1.1

1. Se $n = (a_k a_{k-1} \ldots a_1 a_0)_{10}$ é a representação decimal do natural n, então $n = \sum_{j=0}^{k} a_j 10^j$. Use, agora, o resultado do exemplo 1.4 e o corolário 1.9.

2. Escreva $10^k = (11 - 1)^k$ e desenvolva o binômio do segundo membro.

3. Escreva $n = \sum_{j=0}^{k} a_j 10^j$ e use o resultado do problema anterior, juntamente com o corolário 1.9.

4. Seja $n = (abc)_{10}$ a representação decimal de n; use o resultado do problema anterior para concluir que $a - b + c = 0$ ou 11.

5. Se n tiver k algarismos, use as condições do enunciado para mostrar que $9^k \geq 10^{2(k-1)} - 10^k - 22$ e, daí, concluir que $k = 1$ ou 2.

6. Para $a \in \mathbb{N}$, comece observando que $(a+1)(a+2)\ldots(a+n) = \frac{(a+n)!}{a!}$.

7. Comece mostrando que um número natural é múltiplo de 10 se, e só se, for simultaneamente múltiplo de 2 e de 5. Assim, como o número em questão é claramente par, basta mostrarmos que é um múltiplo de 5; para tanto, use o resultado do exemplo 1.3.

8. Use o resultado do item (b) do exemplo 1.3.

9. No item (c), para mostrar que $S \subset \mathbb{Z}m$, use o algoritmo da divisão e a minimalidade de m.

10. Comece analisando a primeira parte do problema e, para tanto, escreva $2^{64} + 1 = (2^{64} - 1) + 2$ e fatore $2^{64} - 1$.

12. Para os itens de (a) a (e), é suficiente aplicar judiciosamente os itens (a) e (b) do problema anterior. Quanto ao item (f), comece utilizando o resultado do item (b).

13. Comece analisando o caso em que x pertence a um intervalo do tipo $(n, n + \frac{1}{2})$, para algum $n \in \mathbb{Z}$.

14. Comece mostrando que, nas condições do enunciado, temos $\frac{a^2}{b} + \frac{b^2}{a} + 1 > \frac{a^2+b^2}{ab} - 1 + ab$ e, daí, que $1 + (a + b - 1)(a^2 + b^2 - ab) > a^2b^2$. Conclua, por fim, que $a \geq b \Rightarrow b = 1$.

15. Desenvolvendo a igualdade do enunciado, obtemos $(x + y)(x + z) = 2xz$. Conclua que um dos membros dessa última igualdade é um múltiplo de 4, enquanto o outro não o é.

16. Aplique os itens (a) e (b) do corolário 1.8.

17. Para o item (b), use o resultado de (a); quanto a (a), escreva $n = 7q + r$, com $r = 0, 1, 2, 3, 4, 5$ ou 6, e calcule n^3.

18. Certamente $n > 1$ e podemos supor que $x \leq y < z$; se $x = y$, mostre que $n = 2$; se $x < y$, temos $1 = n^{y-x}(n^{z-y} - 1)$.

19. Para $k \geq 5$, mostre que o último algarismo de $k!$ é 0; use, em seguida, o resultado do exemplo 1.10.

20. Use o resultado do exemplo 1.10.

21. Para o item (a), escreva $n = 2^r q$, onde r é um inteiro não negativo e q um natural ímpar. Conclua, então, que $q = 1$.

Seção 1.2

1. Use o algoritmo de Euclides.

2. $2^m = (n - 1)(n + 1)$; calcule, agora, os possíveis valores de $\text{mdc}(n - 1, n + 1)$ e, em seguida, utilize o item (b) do corolário 1.22.

3. Mostre que, se existir um natural que é termo de ambas as PA's, então existirá uma infinidade de naturais que são termos das mesmas; para a caracterização da existência de um natural que seja termo comum das PA's, use a proposição 1.25.

4. Trabalhe novamente o problema 10, página 11.

5. Comece mostrando que o mdc que se quer calcular divide $(n + 1)! - n! = n \cdot n!$.

6. Se $d = \text{mdc}(a, b)$, escreva $a = du$ e $b = dv$, de sorte que $\text{mdc}(u, v) = 1$. Então $ab \mid (a^2 + b^2)$ se, e só se, $uv \mid (u^2 + v^2)$. Nesse caso, como $u, v \mid uv$, temos que $u, v \mid (u^2 + v^2)$ e, daí, $u \mid v^2$ e $v \mid u^2$. Mas, uma vez que $\text{mdc}(u, v) = 1$ implica $\text{mdc}(u, v^2) = \text{mdc}(u^2, v) = 1$, tais relações de divisibilidade implicam $u = v = 1$. Assim, $a = b = d$. Alternativamente, escreva $a^2 + b^2 = abk$, com $k \in \mathbb{N}$, e examine o discriminante da equação de segundo grau $x^2 - (bk)x + b^2 = 0$, a qual tem a raiz natural a.

7. Analise primeiro o caso $\text{mdc}(a, b) = 1$. Nesse caso, mostre que a diagonal principal não pode tocar um quadradinho somente em um vértice e que ela intersecta a coluna de quadradinhos entre $x = j$ e $x = j + 1$ em exatamente $\lfloor \frac{b}{a}(j + 1) \rfloor + 1 - \lfloor \frac{b}{a} j \rfloor$ quadradinhos.

8. Sendo d o mdc procurado, segue do teorema das colunas do triângulo de Pascal – cf. proposição 6.5 do volume 1 – que d divide a soma $\binom{n+k+1}{k+1}$ dos números dados. portanto, d divide $\binom{n+k+1}{k+1} - \binom{n+k}{k} = \binom{n+k}{k+1}$. Conclua, a partir daí e com o auxílio da relação de Stiefel (cf. proposição 6.3 do volume 1), que d divide $\binom{n+1}{k+1}, \binom{n+2}{k+1}, \ldots \binom{n+k}{k+1}$. Por fim, argumente indutivamente.

9. Se d é o mdc dos números binomais dados, então d é uma potência de 2, uma vez que d divide sua soma, a qual vale 2^{2n-1}. Escreva $n = 2^k q$, com $q \in \mathbb{N}$ ímpar, e mostre que
$$\binom{2n}{2t-1} = 2^{k+1} \cdot \frac{(2n-1)q}{(2t-1)(2n-2t+1)} \binom{2n-2}{2t-2};$$
conclua, a partir daí, que 2^{k+1} divide todos os binomiais dados.

10. Se $d = \text{mdc}\,(n^2+k, (n+1)^2+k)$, então $d \mid [((n+1)^2+k) - (n^2+k)]$; logo, $d \mid [(2n+1)^2 - 4(n^2+k)]$, e é fácil concluir, a partir daí, que $d \mid (4k+1)$, de sorte que $d \leq 4k+1$. Exiba, agora, um valor de n para o qual o mdc correspondente seja igual a $4k+1$.

11. Comece escrevendo $a = du$ e $b = dv$, onde $d = \text{mdc}\,(a,b)$ e, por conseguinte, $\text{mdc}\,(u,v) = 1$; conclua, em seguida, que $u, v \mid c$ e, daí, que $uv \mid c$.

12. Faça $x^2 + y^2 - x = 2xym$, com $m \in \mathbb{N}$; em seguida, considerando tal igualdade como uma equação de segundo grau em x, mostre que o fato de x ser inteiro garante que o discriminante $\Delta = (2ym+1)^2 - 4y^2 = (2ym+1-2y)(2ym+1+2y)$ deve ser um quadrado perfeito. Por fim, mostre que $\text{mdc}\,(2ym+1-2y, 2ym+1+2y) = 1$ e use o resultado do corolário 1.22.

13. Mostre inicialmente, com o auxílio do princípio da casa dos pombos – cf. seção 4.1 do volume 4 – que ao menos um dos cinco naturais ímpares em nosso conjunto não é múltiplo de 3, 5 ou 7; em seguida, prove que tal número é primo com os outros nove.

$mdc(y,z) = 1$.

14. Escreva $aj + b = m\lfloor \frac{aj+b}{m} \rfloor + r_j$, com $0 \leq r_j < m$; em seguida, use a condição $\text{mdc}\,(a,m) = 1$ para concluir que $r_0, r_1, \ldots, r_{m-1}$ são dois a dois distintos.

15. Escreva $r = gu$, $n = gv$, com $\text{mdc}\,(u,v) = 1$; em seguida, faça $\{\frac{ui}{v}\} = \frac{ui}{v} - \lfloor \frac{ui}{v} \rfloor$ e use o resultado do problema anterior.

16. Escreva $\text{mdc}\,(m,n) = mx + ny$, com $x, y \in \mathbb{Z}$.

17. Utilize o resultado do item (a) do problema 5.11 do volume 1.

18. Prove o item (a) por indução sobre n e o item (b) por indução sobre k. Quanto ao item (c), para o subitem (i) use (b) para mostrar, também por indução, que $F_n \mid F_{nq}$; para o subitem (ii), use (i) e (a); para (iii), faça uma prova por indução sobre $q \geq 0$, utilizando (b) e (ii) no passo de indução. Por fim, para o item (d), adapte o algoritmo de Euclides à situação em questão, com o auxílio do item (c).

19. Adapte, ao presente caso, os passos e sugestões do problema anterior.

20. Para o item (a), sejam u e v naturais tais que $au - bv = 1$. O fato de ser $n > ab$ nos dá $nau - nbv = n > ab$ e, daí, $\frac{nu}{b} - \frac{nv}{a} > 1$; portanto, existe um inteiro t tal que $\frac{nv}{a} < t < \frac{nu}{b}$; faça $x = nu - bt$ e $y = at - nv$. Agora, obtenha (b) argumentando por contradição e reduza (c) a (a) e (d) a (b). Quanto a (e), faça $S = ab - a - b$ e mostre que, para $0 \leq m \leq S$, exatamente um dos números m e $S - m$ pode ser escrito como pede o enunciado.

21. (a) Sejam $x, y, z \in \mathbb{Z}_+$ tais que $2abc - ab - bc - ca = xbc + yac + zab$. Então
$$2abc = (x+1)bc + (y+1)ac + (z+1)ab$$
e, daí, $a \mid (x+1)bc$. Como $\text{mdc}\,(a, bc) = 1$, segue que $a \mid (x+1)$ e, portanto, $x + 1 \geq a$. Analogamente, $y + 1 \geq b$ e $z + 1 \geq c$. Mas aí,
$$(x+1)bc + (y+1)ac + (z+1)ab \geq a \cdot bc + b \cdot ac + c \cdot ab = 3abc,$$
o que é uma contradição. (b) Se $n > 2abc - ab - bc - ca$, então $n > a \cdot bc - a - bc$ e o problema anterior garante (a e bc são primos entre

si) a existência de inteiros $x, t \in \mathbb{Z}_+$ tais que $n = xbc + ta$. Sem perda de generalidade, podemos supor que $0 \le x < a$. De fato, se $x \ge a$ escreva $x = aq + x'$, com $0 \le x' < a$, obtendo $n = x'bc + (t + qbc)a$. (c) Sendo $x \le a - 1$, temos

$$ta = n - xbc \ge (2abc - ab - bc - ca) - (a-1)bc = abc - ab - ac,$$

donde $t > bc - b - c$. Mas, como b e c são primos entre si, novamente pelo resultado do problema anterior existem $y, z \in \mathbb{Z}_+$ tais que $t = bz + cy$. (d) Nas notações dos itens anteriores, temos

$$n = xbc + ta = xbc + (bz + cy)a = xbc + yac + zab.$$

22. Adapte os passos descritos no problema anterior e faça indução sobre $n \ge 2$.

23. Para a primeira parte do item (a), use indução. Para o item (b), mostre que, se $0 < a_1 < a_2 < a_3 < \cdots < a_{n-1}$ são os restos obtidos na execução do algoritmo de Euclides para o cálculo do mdc de $a = a_{n+1}$ e $b = a_n$ (sendo a_{n-1} o primeiro resto, etc, a_1 o último), então $a_j \ge F_{j-1}$, para $1 \le j \le n$. Por fim, mostre que (c) segue de (a) e de (b).

24. Sejam k o único inteiro positivo tal que $2^k \le n < 2^{k+1}$ e $M = \text{mmc}\,(1, 2, \ldots, n)$. Mostre que $2^k \mid M$ e que

$$\sum_{j=1}^{n} \frac{1}{j} = \frac{1}{M} \sum_{j=1}^{n} \frac{M}{j},$$

com $\frac{M}{j}$ ímpar se, e só se, $j = 2^k$.

Seção 1.3

1. Use o fato de que $p + q$ é par e, se $p < q$, então $p < \frac{p+q}{2} < q$, de sorte que $(p+q)/2$.

2. Comece escrevendo $\frac{m}{n} = \sum_{j=1}^{2k+1} \frac{1}{j} - 2\sum_{j=1}^{k} \frac{1}{2j} = \sum_{j=k+1}^{2k+1} \frac{1}{j}$; em seguida, agrupe as parcelas dessa última soma de duas em duas, para escrevê-la como uma soma de frações com numeradores todos iguais a $3k + 2 = p$, e use o fato de p ser primo.

3. Podemos supor $x \ne y$. Se $x < y$, prove que $x < p < y$ e, daí, que $\text{mdc}\,(p, x) = 1$. Escreva $2xy = p(x + y)$ para concluir que $p \mid y$. Faça $y = pz$ para obter $z = \frac{x}{2x-p}$, concluindo, daí, que $(2x - p) \mid 2x$ e, então, que $(2x - p) \mid p$.

4. Comece considerando separadamente os casos $n = 6k, 6k+1, \ldots, 6k+5$. Para $n = 6k$, por exemplo, use o fato de que k, $2k + 1$, $3k + 1$ e $6k + 1$ são dois a dois primos entre si para concluir que $k = 1$.

5. Comece utilizando a condição do enunciado para mostrar que $n \mid a_n$ e, daí, que se p é um primo que não divide n, então $p \nmid a_n$.

6. Para o item (a), use o teorema fundamental da aritmética (para cuja prova não utilizamos a infinitude dos primos). Para a primeira parte do item (b) use, além do resultado do item (a), o princípio fundamental da contagem. Por fim, mostre que o resultado de (b) gera a desigualdade $n \le 2^k \sqrt{n}$, a qual, por sua vez, gera uma contradição.

7. Em cada um dos casos em questão, imite a ideia da prova do exemplo 1.39. Para tanto, observe que todo primo $p \ne 3$ é da forma $3k \pm 1$ e todo primo $p \ne 2, 3$ é da forma $6k \pm 1$.

8. Fatore $2^{2^n} - 1$ e use o resultado do problema 4, página 31.

9. Use a identidade de Lagrange – cf. exemplo 6.12 do volume 1 ou exemplo 2.8 do volume 4 – para escrever $\binom{2p}{p}$; em seguida, use o resultado do exemplo 1.41. Alternativamente, escreva

$$\binom{2p}{p} - 2 = \frac{(p+1)(p+2)\ldots(2p-1)}{1 \cdot 2 \ldots (p-1)} - 1$$

e mostre que p divide $(p+1)(p+2)\ldots(2p-1) - 1 \cdot 2 \ldots (p-1)$.

10. Para o item (a), mostre que, se n não for uma potência de 2, então é possível fatorar $a^n + 1$; argumente analogamente quanto ao item (b).

11. Considere separadamente os casos n par e n ímpar; no caso $n = 4k$, calcule mdc $\left(\frac{n}{2} - 1, n\right)$; no caso $n = 4k + 2$, calcule mdc $\left(\frac{n}{2} - 2, n\right)$; por fim, no caso n ímpar, calcule mdc $\left(n, \frac{n+1}{2}\right)$.

12. Fatore $c_{m+j} - c_k$ e, em seguida, aplique o resultado do problema 6, página 10.

13. Se $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ é a fatoração canônica de n, escreva $u = p_1^{\beta_1} \ldots p_k^{\beta_k}$ e $v = p_1^{\gamma_1} \ldots p_k^{\gamma_k}$, com $\beta_i, \gamma_i \geq 0$, e calcule quantos são os pares ordenados (β_i, γ_i) tais que $\max\{\beta_i, \gamma_i\} = \alpha_i$. Aplique, em seguida, o corolário 1.47.

14. Escreva $\frac{a}{b^2} = \frac{c}{d}$, com mdc $(c, d) = 1$, e deduza que $b = x^d$ e $a = x^c$, para algum $x \in \mathbb{N}$. Conclua, então, que $x = 1$ ou $cx^{2d} = dx^c$; no segundo caso, analise separadamente os subcasos $c < 2d$, $c = 2d$ e $c > 2d$.

15. Se n for ímpar, então não há soluções, uma vez que ambos os membros da igualdade do enunciado têm paridades distintas. Se n for par, então $n = 5 + d_3^2 + d_4^2$, com d_3 e d_4 com paridades distintas. Se n for múltiplo de 4, mostre que $n = p^2 + 21$, onde p é o menor primo ímpar que divide n e, então, que $p \mid 21$; conclua que não há soluções nesse caso. Se n for da forma $4k + 2$, mostre que $n = 5(p^2 + 1)$, onde p é o menor primo ímpar que divide n. Conclua, a partir daí, que $p = 5$ e, então, que $n = 130$.

16. Sendo $n = d_{13}q_{13} = d_{14}q_{14} = d_{15}q_{15}$, com $q_{13}, q_{14}, q_{15} \in \mathbb{N}$, a condição (b) equivale a $\frac{1}{q_{13}} + \frac{1}{q_{14}} + \frac{1}{q_{15}} = 1$; comece, então, obtendo todos os $a < b < c$ naturais tais que $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$.

17. Examinando os casos $1 \leq n \leq 30$, conjecture que os naturais n da forma $2^k - 2$ satisfazem a propriedade do enunciado. Em seguida, prove esse resultado escrevendo, para $n = 2^k - 2$,

$$\begin{aligned} I(n) &= \sum_{j=1}^{2^{k-1}-1} d(2j-1) + \sum_{i=1}^{k-1} \Big(d(2^i) + d(2^i \cdot 3) + \cdots + d(2^k - 2^i) \Big) \\ &= \left(2^{k-1} - 1\right)^2 + \sum_{i=1}^{k-1} \Big(1 + 3 + 5 + \cdots + (2^{k-i} - 1) \Big) \\ &= \left(2^{k-1} - 1\right)^2 + \sum_{i=1}^{k-1} 2^{2k-2i-2} \\ &= \left(2^{k-1} - 1\right)^2 + \frac{2^{2k-2} - 1}{3} = \frac{(2^k - 2)(2^k - 1)}{3}. \end{aligned}$$

18. Veja que $3 \mid n$. Escreva $n = 2^\alpha \cdot 3^\beta p_1^{k_1} \cdots p_t^{k_t}$, onde $3 < p_1 < \cdots < p_t$ são primos e $\alpha \geq 0$, $\beta \geq 1$, e note que a relação do enunciado se reduz à equação $3(\alpha + 1)(\beta + 1)(k_1 + 1) \cdots (k_t + 1) = 2^\alpha 3^\beta p_1^{k_1} \cdots p_t^{k_t}$, Conclua, a partir daí, que $\beta = 1$ ou 2 e que n não possui outros fatores primos; em seguida, analise cada um de tais casos.

19. Fixado um primo p qualquer, basta mostrar que $e_p(2m) + e_p(2n) \geq e_p(m) + e_p(n) + e_p(m + n)$. Para tanto, use a fórmula de Legendre e o item (f) do problema 12, página 11.

20. Para o item (a), use a fórmula de Legendre para mostrar que $e_2(2n) \geq 2e_2(n) + 1$, para todo $n \in \mathbb{N}$ – alternativamente, veja o problema 6.2.18 do volume 1. Para o item (b), refine os cálculos do item (a) para mostrar que $e_2(2n) \geq 2e_2(n) + 2$ se, e só se, n não for uma potência de 2.

21. Escreva $n = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_m 2^m$, com $a_j \in \{0, 1\}$ para $0 \leq j \leq m$, de sorte que $a_0 + a_1 + \cdots + a_m = k$. Calcule

$$\left\lfloor \frac{n}{2^j} \right\rfloor = a_j + a_{j+1} \cdot 2 + \cdots + a_m \cdot 2^{m-j}$$

e, em seguida, use a fórmula de Legendre para mostrar que $e_2(n) = n - k$.

22. Sejam p primo e $t \in \mathbb{N}$ tais que $(a+kb)(b+ka) = p^t$. Supondo, sem perda de generalidade, que $a \leq b$, temos $a + kb \geq b + ka > 1$, de sorte que existem $r, s \in \mathbb{Z}$ tais que $1 \leq r \leq s$, $r + s = t$ e $a + kb = p^s$ e $b + ka = p^r$. Conclua que $(b + ka) \mid (a + kb)$ e, escrevendo $\frac{a+kb}{b+ka} = k - \frac{(k^2-1)a}{b+ka}$, que $(b + ka) \mid (k^2 - 1)$. Considere, agora, dois casos separadamente: (i) se $p > 2$, use o fato de que $b + ka$ é uma potência de p e $\text{mdc}\,(k-1, k+1) \leq 2$ para concluir que $b + ka$ divide $k - 1$ ou $k + 1$, de sorte que $b + ka \leq k + 1$ e, então, $b = a = 1$. Conclua que, nesse caso, as soluções são os ternos $(a, b, k) = (1, 1, p^r - 1)$, para todos $r \geq 1$ e $p > 2$ primo. (ii) Se $p = 2$, comece observando que ao menos um dentre a e b é ímpar e, portanto, que k também é ímpar. Agora, como $(b+ka) \mid (k^2-1)$ e $b+ka = 2^r$, mostre que $(b+ka) \mid 2(k+1)$ ou $2(k-1)$; em particular, $b+ka \leq 2k+2$ e, daí, $a = 1$ ou 2. Se $a = 2$, chegue a uma contradição; se $a = 1$, temos que $(b + k) \mid 2(k + 1)$ ou $k - 1$, o que suscita a análise de dois subcasos: $(b+k) \mid (2k+2)$ ou $(b+k) \mid (2k-2)$. No primeiro subcaso, mostre que $b = k + 2$ ou $b = 1$. Se $b = 1$, conclua que $k = 2^r - 1$; se $b = k + 2$, escreva $s = 2u$ para obter $(a, b, k) = (1, 2^u + 1, 2^u - 1)$, para todo $u \in \mathbb{N}$. No segundo subcaso, mostre que $b = k - 2$ e, em seguida, faça $s = 2u$ para obter $(a, b, k) = (1, 2^u - 1, 2^u + 1)$, para todo $u \in \mathbb{N}$.

23. Para o item (a), use o resultado do problema 4, página 31, juntamente com o fato de que $p(q^{2^k}) = q$, para todo $k \geq 0$. Para o item (b), fatore $q^{2^k} - 1$ e use a minimalidade de k para concluir que não pode ser $p(q^{2^{k-1}} - 1) > p(q^{2^{k-1}})$.

24. Escolha um primo p maior que $1 + 2 + \cdots + 1000$ e mostre que o conjunto $A = \{p, 2p, 3p, \ldots, 1000p\}$ satisfaz as condições do enunciado.

25. Se t é o produto dos primos menores ou iguais a m, defina $y_1 = x_{t_1}$, onde p_{t_1} é um primo maior que t. Sendo p o maior divisor primo de y_1 e $p = p_r$ na sequência dos primos, defina $y_2 = x_{t_2}$, com $t_2 > r, t_1$, e se convença de que $\text{mdc}\,(y_1, y_2) = 1$. Escolhidos elementos $y_1 = x_{t_1} < \cdots < y_j = x_{t_j}$ de A satisfazendo a condição do item (b), com $j < m$, seja p o maior fator primo de y_j e $p = p_r$ na sequência dos primos; defina $y_{j+1} = x_{t_{j+1}}$, com $t_{j+1} > r, t_j$. Prossiga dessa maneira até que $j = m$, mostrando, em seguida, que o conjunto B assim obtido também satisfaz a condição (c).

Seção 2.1

1. Se (x_0, y_0, z_0) é uma solução, então $(x_0 a^{n+1}, y_0 a^{n+1}, z_0 a^n)$ também é solução; agora, obtenha uma solução com $x = y = k + 1$.

2. Use a proposição 2.1 para escrever $x + y$, $y + z$ e $x + z$ em termos de parâmetros u, v e d, como prescrito por aquele resultado.

3. Imite a prova da proposição 2.1. Mais precisamente, se $x, y, z > 0$, comece observando que $z - x$ e $z + x$ são ambos pares e, se $d = \text{mdc}\left(\frac{z-x}{2}, \frac{z+x}{2}\right)$, então a igualdade

$$\left(\frac{z-x}{2d}\right)\left(\frac{z+x}{2d}\right) = 2\left(\frac{y}{d}\right)^2$$

garante a existência de $u, v \in \mathbb{Z}$ tais que $\frac{z-x}{2d} = 2v^2$, $\frac{z+x}{2d} = u^2$; agora, mostre que $\text{mdc}\,(u, 2v) = 1$.

4. Use o método da descida de Fermat em cada um dos itens acima, nos moldes dos exemplos 2.3 e 2.4. Especificamente para o item (d), comece mostrando que x e y deixam restos iguais quando divididos por 3; em seguida, calculando $(3k + r)^3$, conclua que, se x e y não forem múltiplos de 3, então $x^3 + 5y^3$ não será múltiplo de 9.

5. Comece escrevendo $x = u - v$ e $y = u + v$, com $u, v \in \mathbb{Q}$ e, em seguida, $u = \frac{a}{c}$ e $v = \frac{b}{c}$, com $a, b, c \in \mathbb{Z}$ e $\text{mdc}\,(b, c) = 1$. Em seguida, para o item (a) utilize o resultado do exemplo 2.3; para o item (b), adapte a demonstração da proposição 2.1 para resolver a equação $3a^2 + b^2 = c^2$.

6. Se z for ímpar, use o resultado do item (c) do corolário 1.8 para mostrar que não há soluções. Se z for par, use o item (b) do mesmo

resultado para concluir que w, x e y também são pares e, em seguida, aplique o método da descida de Fermat.

7. Multiplique a igualdade do enunciado por 4, complete quadrados e reduza $2x+3$, $2y+3$ e $2z+3$ a um mesmo denominador comum para reduzir o problema em questão ao problema anterior.

8. Se a e b são os catetos e c é a hipotenusa de um desses triângulos, então o teorema de Pitágoras nos dá $a^2+b^2=c^2$; por outro lado, o resultado da proposição 3.37 do volume 2 fornece a relação $a+b-c=2r$. Use as fórmulas da proposição 2.1 na primeira igualdade, substituindo-as, em seguida, na segunda igualdade para obter $v(u-v)=r$; a partir daí, mostre que $\mathrm{mdc}\,(v,u-v)=1$ e conclua que há 2^k escolhas possíveis para v, após o quê u estará completamente determinado. Para ver que os triângulos assim obtidos são dois a dois não congruentes, veja que
$$c^2=u^2+v^2=\left(v+\frac{r}{v}\right)^2+v^2=2v^2+\frac{r^2}{v^2}+2r,$$
com $2v_1^2+\frac{r^2}{v_1^2}=2v_2^2+\frac{r^2}{v_2^2}$ se, e só se, $v_1=v_2$.

9. Comece fazendo A_1A_2 igual a um diâmetro do círculo; em seguida, use (2.1) para escolher pontos $A_3, \ldots, A_n$ tais que A_1A_i e A_2A_i sejam racionais, para $3\leq i\leq n$; por fim, use o teorema de Ptolomeu (teorema 4.17 do volume 2) para mostrar que A_iA_j também é racional.

Seção 2.2

1. Substitua $d=4k+3$, $m=4l+3$ e use o corolário 1.8.

3. Imite a discussão do exemplo 2.6, observando que $x=y=1$ é uma solução da equação.

4. Multiplique a igualdade $n^2+(n+1)^2=m^2$ por 2, complete quadrados e use o resultado do problema anterior.

5. Se $x^2-dy^2=m$ e $a^2-db^2=1$, com $a,b\in\mathbb{N}$, então
$$(a-b\sqrt{d})(x_0+y_0\sqrt{d})\cdot(a+b\sqrt{d})(x_0+y_0\sqrt{d})=m$$
ou, ainda,
$$[(ax_0+bdy_0)-(ay_0+bx_0)\sqrt{d}][(ax_0+bdy_0)+(ay_0+bx_0)\sqrt{d}]=m,$$
de sorte que $x_1=ax_0+bdy_0$ e $y_1=ay_0+bx_0$ também resolvem a equação do enunciado. Observe, agora, que
$$x_1^2+dy_1^2=(a^2+db^2)(x_0^2+dy_0^2)+4abx_0y_0d>x_0^2+dy_0^2,$$
de sorte que $(x_1,y_1)\neq(x_0,y_0)$.

6. Completando quadrados, conclua que a equação dada é equivalente à equação $(2x+y)^2-5y^2=4$. Use, agora, o resultado do problema anterior, observando que $x=y=1$ é uma solução da equação original.

7. Imitando o argumento do problema 5, mostre que, se $u,v\in\mathbb{N}$ são tais que $u^2-\Delta v^2=1$, então $\alpha:=ux_0-\Delta vy_0$ e $\beta=uy_0-vx_0$ é solução inteira de $x^2-\Delta y^2=4an$. Agora, observe que
$$ax^2+bxy+cy^2=n\Rightarrow(2ax+by)^2-\Delta y^2=4an,$$
de sorte que, para gerar uma solução inteira da equação $ax^2+bxy+cy^2=n$, é suficiente mostrar ser possível resolver, em $\mathbb{Z}$, o sistema linear
$$\begin{cases}2ax+by=\alpha\\ y=\beta\end{cases}.$$
Tal tarefa, por sua vez, equivale a mostrar que $2a\mid(\alpha-d\beta)$, o que pode ser feito escrevendo
$$\begin{aligned}\alpha-d\beta&=(ux_0-\Delta vy_0)-b(uy_0-vx_0)\\&=u(x_0-by_0)+bv(x_0-by_0)+4acvy_0,\end{aligned}$$
expressão que é igual a uma soma de múltiplos de $2a$.

Capítulo 3

2. Prove primeiro que $\prod_{0<d|n} d = \prod_{0<d|n} \frac{n}{d}$. Em seguida, denote tal produto por P e use essa igualdade para mostrar que $P^2 = n^{d(n)}$.

3. Para $0 < d \mid n$, temos $d + \frac{n}{d} \geq 2\sqrt{n}$. Agora, some tais desigualdades sobre todos os divisores positivos de n.

4. Para a segunda equação, mostre que um par (x, y) é solução se, e só se, $x = n - \frac{n^2}{n+y}$, de modo que $n + y$ deve ser um divisor de n^2 maior que n; utilize agora o exemplo 1.46 e (3.3) para concluir que que há exatamente $\frac{1}{2}(d(n^2) - 1)$ possibilidades para y e, portanto, para (x, y). Quanto à primeira equação, imite a sugestão apresentada para a segunda equação para concluir que há $d(n^2)$ soluções. Por fim, some os números de soluções das duas equações para obter a equação $3d(n^2) = 157$, a qual não possui soluções.

5. Para o item (a), use o resultado do lema 3.3. Para o item (b), se $\text{mdc}\,(m, n) = 1$, use o resultado do item (a) para calcular $|D_1(mn)| - |D_3(mn)|$ em função de $|D_1(m)| - |D_3(m)|$ e $|D_1(n)| - |D_3(n)|$. Por fim, aplique indução.

6. Para o item (a), multiplique ambos os membros da igualdade desejada por n. Para o item (b), calcule diretamente a soma dos divisores positivos de $2^{p-1}(2^p - 1)$.

7. A segunda parte de (b) utiliza o item (b) do problema 10, página 48.

8. Mostre que $s(ab) \geq s(a)b$, para todos $a, b \in \mathbb{N}$. Para tanto, exiba, em função dos divisores positivos de a, um conjunto de divisores positivos de ab cuja soma seja igual a $s(a)b$.

9. Aplique a proposição 3.4.

10. Aplique a proposição 3.4.

11. Conclua, a partir da proposição 3.4 e do problema 1, que ambos os membros da igualdade acima podem ser vistos como funções aritméticas multiplicativas, F e G digamos. Em seguida, se p é primo e $\alpha \in \mathbb{N}$, mostre que $F(p^\alpha) = G(p^\alpha)$.

12. Aplique contagem dupla – cf. seção 2.2 do volume 4 –, mostrando inicialmente que, para $1 \leq j \leq n$, o primeiro membro conta $f(j)$ exatamente $\lfloor \frac{n}{j} \rfloor$ vezes.

13. Comece aplicando o resultado do problema anterior; em seguida, aplique a proposição 3.4 para mostrar que $F(m) = 1$ se m for um quadrado perfeito e $F(m) = 0$ caso contrário.

14. Se $f(j) = 1$ para $j \in \mathbb{N}$ e $F(n) = \sum_{0<d|n} f(d)$, então $F(n) = d(n)$, para $n \in \mathbb{N}$. Agora, aplique o resultado do problema 12.

15. Use a fórmula de inversão de Möbius e o resultado do problema 1.

17. Use o resultado da proposição 3.4.

18. Comece provando que, fixado um divisor positivo d de m, há exatamente $\frac{m}{d} \cdot \varphi(d)$ pares ordenados (d, n) como pede o enunciado. Em seguida, o resultado do corolário 3.13.

20. Para (a), use o item (a) do problema 19. Para (b), escreva $S_m(n) = \sum_{i=1}^{k}(n - a_i)^m$ e desenvolva o binômio $(n - a_i)^m$. Para a primeira parte de (c), use (b); quanto à segunda parte, considere separadamente os casos n par e n ímpar e aplique a conclusão do item (a) no caso em que n é par.

21. Para o item (a), escolha d de tal forma que $\text{mdc}\,(m, n) = \frac{n}{d}$ e a tal que $m = \frac{n}{d} \cdot a$; conclua, então, que $\text{mdc}\,(a, d) = 1$. Para o item (b), use o resultado de (a) para mostrar que $\sum_{0<d|n} \left(\frac{n}{d}\right)^k S_k(d) = 1^k + 2^k + \cdots + n^k$. Para o item (c), aplique a fórmula de inversão de Möbius ao resultado do item (b). Por fim, para os itens (d) e (e), use a fórmula do item (c).

Seção 4.1

1. Use o teorema do número primo.

2. Use o lema 4.3 em conjunção com (4.4).

3. Use o lema 4.3 e o teorema 4.7.

4. Para a primeira parte do item (a), use o fato de que, se $n < p \leq 2n$, com p primo, então $\text{mdc}\,(n!, p) = 1$; para a segunda parte, use a fórmula do desenvolvimento binomial. Para o item (b) use (a), juntamente com o fato de que o número de primos p tais que $n < p \leq 2n$ é exatamente $\pi(2n) - \pi(n)$. Para a segunda parte do item (d), use o fato de que $\frac{x}{2} \geq x^{2/3}$ e $x + 2 \leq \frac{5x}{4}$ para $x \geq 8$. Para o item (d), verifique os casos $2 \leq n \leq 8$ diretamente; em seguida, prove os demais casos por indução sobre $n \geq 8$. Por fim, para o item (e), use os itens (c) e (d), juntamente com a desigualdade (óbvia) $\pi(x) \leq 2\lfloor\frac{x}{2}\rfloor + 2$.

Seção 4.2

1. Pelo teorema de Chebyschev, há pelo menos um primo entre p_n e $2p_n$.

2. Se p é o maior primo que é menor ou igual a n, utilize o teorema de Chebyschev para mostrar que $2p > n$.

3. Se $n = 2k$, escreva $1!2! \ldots n! = 2^k k!(3!5! \ldots, (2k-1)!)^2$ e, em seguida, aplique o resultado do problema anterior. O caso $n = 2k + 1$ pode ser tratado de modo análogo.

4. Se p e q denotam os maiores primos respectivamente menores ou iguais a m e a n, use o resultado do problema 2 para comparar as maiores potências de p e de q em ambos os membros da equação dada.

5. Comece utilizando o resultado do problema 2 para mostrar que $n = p$, um número primo, para o quê siga uma argumentação análoga à delineada na sugestão ao problema anterior. Em seguida, se q é o maior primo menor ou igual a $p-1$, conclua que $m \geq 2q$. Por fim, use a observação que antecede o enunciado deste problema para concluir que $q \leq 5$ e, portanto, que $p - 1 \leq 6$. As soluções são $m = n = 2$ ou $m = 10$, $n = 7$.

6. Sejam $n > 1$ um natural satisfazendo as condições do enunciado e $p < \sqrt{n}$ um número primo. Então $p \mid n$, pois, do contrário, teríamos $p^2 < n$ e $\text{mdc}\,(n, p^2) = 1$. Assim, n é divisível por $p_1, \ldots, p_k$, onde $p_1 < \cdots < p_k$ são os primos menores que $\sqrt{n}$. Agora, seja $l \in \mathbb{N}$ tal que $2^l \leq \sqrt{n} < 2^{l+1}$. Como, para todo inteiro $k > 1$, há pelo menos dois primos entre 2^k e 2^{k+1}, temos que

$$p_1 \ldots p_k \geq 2(2^2 \ldots 2^{l-1})^2 = 2^{l^2}.$$

Assim,

$$2^{l^2} \leq p_1 \ldots p_k \leq n < 2^{2l+2},$$

de forma que $l \leq 2$. Há, pois, três casos a considerar:

(i) $l = 0$: nesse caso, temos $1 \leq n < 4$, e é imediato verificar que $n = 2, 3$ são soluções.

(ii) $l = 1$: temos que $4 \leq n < 16$ e $2 \mid n$, de forma que $n \in \{4, 6, 8, 10, 12, 14\}$. Uma rápida inspeção garante que as soluções são $n = 4, 6, 8$ ou 12.

(iii) $l = 2$: temos, nesse caso, que $16 \leq n < 64$ e $2, 3 \mid n$. Portanto, $n \in \{18, 24, 30, 36, 42, 48, 54, 60\}$. Novamente uma inspeção simples dessas possibilidades fornece as soluções: $n = 18$, 24 ou 30.

Seção 5.1

1. Argumente por indução sobre m.

3. Use congruências para calcular o resto da divisão do número dado por 4. Em seguida, aplique o resultado da proposição 5.9.

4. Para $k \in \mathbb{Z}_+$, mostre que $7^{4k} \equiv 1 \pmod{10}$, $7^{4k+1} \equiv 7 \pmod{10}$, $7^{4k+2} \equiv -1 \pmod{10}$ e $7^{4k+3} \equiv 3 \pmod{10}$; em seguida, calcule o resto da divisão de 3^{10} por 4.

5. Se todos os divisores primos de n fossem congruentes a 1, módulo 4, use as propriedades elementares de congruências para concluir que deveríamos ter $n \equiv 1 \pmod 4$.

6. A primeira igualdade nos dá $2^{32} + 2^{28} \cdot 5^4 \equiv 0 \pmod{641}$; a segunda, $2^{28} \cdot 5^4 \equiv (-1)^4 \pmod{641}$.

7. Suponha que a representação decimal de n tenha $k + 1$ algarismos e seja m o natural formado pelos k primeiros algarismos de n. Mostre que a condição do enunciado equivale à igualdade $6 \cdot 10^k + m = 4(10m + 6)$ ou, ainda, $3 \cdot 10^k = 13m + 12$; a partir daí, conclua que basta encontrar os naturais k tais que $10^k \equiv 4 (\text{mod}\, 13)$.

8. Comece observando que $2^n + 3^n \equiv 0 \pmod 7$ se, e só se, $6^n + 9^n \equiv 0 \pmod 7$, o que, por sua vez, equivale a $(-1)^n + 2^n \equiv 0 \pmod 7$. Em seguida, calcule as possíveis congruências de 2^n, módulo 7.

10. Use congruências para mostrar que os restos das divisões dos números de Fibonacci por 5 formam uma sequência periódica.

11. Use congruência módulo 3 para mostrar que p ou q deve ser múltiplo de 3 e, daí, igual a 3; em seguida, supondo $q = 3$, escreva $p^2+9p+9 = n^2$ e resolva tal igualdade para p.

    Aplique o item (e) da Proposição 5.9.

13. Use módulo 3 para concluir que m é par. Em seguida, fatore $k^2 - 2^m$ e argumente como no exemplo 5.11.

14. Se $n \geq 5$, conclua que $m^p \equiv 3 \pmod{10}$ e, daí, que $p > 2$. Em seguida, use módulo 3 para concluir que $3 \mid m$ e, portanto, que $27 \mid m^p$. Por fim, use módulo 27 para concluir que não há soluções quando $n \geq 9$.

15. Use módulo 3 para mostrar que z é par, digamos $z = 2t$; em seguida, fatore $5^{2t} - 4^y$ e argumente como no exemplo 5.11.

16. Se $y = 1$, então $p = 2$ e $x = 1$; se $y > 1$, escreva $p^x = (y+1)(y^2-y+1)$ e mostre que, se $d = \text{mdc}\,(y + 1, y^2 - y + 1)$, então $d = 1$ ou 3. Por fim, considere separadamente os casos $d = 1$ e $d = 3$.

17. Escreva $a = 2^k\alpha$ e $b = 2^l\beta$, com $k, l \geq 1$ e α, β ímpares. Mostre, a partir daí, que $kb = la$ e $\alpha^b+\beta^a = 2^{c-kb}$, e use módulo 4 para concluir que $\alpha = \beta = 1$ e $\frac{k}{2^k} = \frac{l}{2^l}$. Por fim, analisando a função $f(x) = \frac{x}{2^x}$, mostre que, se $k, l \geq 4$, então $k = l$.

18. Inicialmente, mostre que basta considerar o caso $b = a^n$. Para tal caso, faça indução sobre $n \geq 0$, utilizando congruência módulo a no passo de indução.

19. Comece analisando a equação, módulo 3, para concluir que b é par. Em seguida, faça $b = 2c$ e conclua que $2^{c+1} = 15^a + 1$ ou $2^{c+1} = 3^a + 5^a$. Faça $d = c + 1$ e, no primeiro caso, use módulo 3 para concluir que d é par e, em seguida, que $2^{d/2} - 1 = 3^a$ e $2^{d/2} + 1 = 5^a$. No segundo caso, use módulo 4 para concluir que a é ímpar, de sorte que, se $c - 2 > 0$, temos

$$2^{c-2} = 3^{a-1} - 3^{a-2} \cdot 5 + \cdots + 5^{a-1} \equiv a \pmod 2;$$

    conclua, pois, que $c - 2 = 0$.

20. Utilizando o fato de que $1992 = 24 \cdot 83$, mostre que o resto da divisão de 10^{1992} por $10^{83} + 7$ é 7^{24}. Em seguida, se $q \in \mathbb{N}$ é tal que $10^{1992} = (10^{83} + 7)q + 7^{24}$, use congruências módulo 10 para calcular o último algarismo de q.

Seção 5.2

1. Use o pequeno teorema de Fermat com $p = 7$.

2. Considere, inicialmente, os casos $p = 2, 3, 5$. Se $p \neq 2, 3, 5$, escreva a diferença acima como

$$(a \cdot 10^{8p} - 10^8) + 2(a \cdot 10^{7p} - 10^7) + \cdots + 9(a - 1),$$

onde $a = \underbrace{11\ldots1}_{p}$; em seguida, aplique o pequeno teorema de Fermat para concluir que $a \equiv 1 \pmod p$ e para analisar o resto da divisão de cada parcela da soma acima por p.

3. Mostre que, módulo $2n+1$, o $j-$ésimo termo da sequência vai para a posição $2^k j$ após $k \geq 1$ operações; em seguida, use o pequeno teorema de Fermat.

4. Inicialmente, use módulo 11 para concluir que não há soluções tais que $x \equiv 0 \pmod{11}$; se $x \not\equiv 0 \pmod{11}$, use o pequeno teorema de Fermat para concluir que 11 divide $x^5 + 1$ ou $x^5 - 1$ e, daí, que $y^2 \equiv -5$ ou $-3 \pmod{11}$. Por fim, mostre que tais congruências não têm soluções.

5. Podemos supor $p > 2$; nesse caso, se $n = pq + r$, o pequeno teorema de Fermat garante que basta encontrarmos um inteiro $0 \leq r < p$ tal que $2^{q+r} \equiv r \pmod p$ para infinitos naturais q. Escolha $r = 1$ e, a partir daí, infinitos q's.

6. Suponha que exista um inteiro $n > 1$ tal que $n \mid (3^n - 2^n)$. Se p é o menor fator primo de n, com $n = mp$, use o pequeno teorema de Fermat para concluir que $3^m \equiv 2^m \pmod p$. Em seguida, use a minimalidade de p para concluir que $\text{mdc}\,(m, p-1) = 1$. Por fim, escreva $mx = (p-1)y + 1$, com $x, y \in \mathbb{N}$, e use novamente o pequeno teorema de Fermat para chegar a uma contradição.

7. Para o item (b), comece usando o fato de que $\text{mdc}\,(p, q-1) = 1$ para escrever $px = (q-1)y + 1$, com $x, y \in \mathbb{N}$. Em seguida, use o pequeno teorema de Fermat.

8. Se k é o número de algarismos de 5^n, mostre que a condição do enunciado equivale a $5^m - 5^n \equiv 0 \pmod{10^k}$; prove que $n \geq k$ e conclua, a partir daí, que devemos ter $5^{m-n} \equiv 1 \pmod{2^k}$. Use, então, o teorema de Euler.

9. Com a ajuda do teorema de Euler, prove primeiro que, se l for ímpar, então $\text{mdc}\,(2^{\varphi(l)m} - 3, l) = 1$, para todo $m \in \mathbb{N}$; em seguida, escolha $k_1, \ldots, k_n$ indutivamente.

10. Use a fórmula de inversão de Möbius para obter $a_n = \sum_{0<d|n} \mu(d) 2^{\frac{n}{d}}$. Em seguida, use o teorema de Euler para mostrar que, se p é primo e p^α é a maior potência de p que divide n, então $p^\alpha \mid a_n$. Para tal fim, escreva $n = p^\alpha k$, com $\text{mdc}\,(k, p) = 1$, e, a partir daí,

$$\begin{aligned}
a_n &= \sum_{0<d|p^\alpha k} \mu(d) 2^{\frac{p^\alpha k}{d}} = \sum_{0<d|k} \mu(d) 2^{\frac{p^\alpha k}{d}} + \sum_{0<d|k} \mu(pd) 2^{\frac{p^\alpha k}{pd}} \\
&= \sum_{0<d|k} \mu(d) 2^{\frac{p^\alpha k}{d}} - \sum_{0<d|k} \mu(d) 2^{\frac{p^{\alpha-1} k}{d}} \\
&= \sum_{0<d|k} \mu(d) \left\{ \left(2^{\frac{p^{\alpha-1}k}{d}}\right)^p - 2^{\frac{p^{\alpha-1}k}{d}} \right\} \\
&= \sum_{0<d|k} \mu(d) 2^{p^{\alpha-1} \cdot \frac{k}{d}} \left(2^{\frac{p^{\alpha-1}(p-1)k}{d}} - 1\right) \\
&= \sum_{0<d|k} \mu(d) 2^{p^{\alpha-1} \cdot \frac{k}{d}} \left(2^{\varphi(p^\alpha) \cdot \frac{k}{d}} - 1\right).
\end{aligned}$$

11. Para o item (a), argumente por contradição. Mais precisamente, se $a = (p_1 - 1) \ldots (p_k - 1)$, com $k \geq 1$ mínimo como em (a), use que $\text{mdc}\,(2^{a/2} - 1, 2^{a/2} + 1) = 1$ para concluir que existem $l < k$ primos dentre $p_1, \ldots, p_k$, digamos $p_1, \ldots, p_l$, tais que $2^{a/2} - 1 = p_1^{\alpha_1} \ldots p_l^{\alpha_l}$; em seguida, se $b = (p_1 - 1) \ldots (p_l - 1)$, use o fato de $(2^b - 1) \mid (2^{a/2} - 1)$ para contradizer a minimalidade de k.

12. Para o item (b), use o pequeno teorema de Fermat. Para (f), se $q \nmid x$, mostre que $x^{(q-1)/2} \equiv \pm 1 \pmod q$, e analogamente para $y^{(q-1)/2}$ e $z^{(q-1)/2}$; em seguida, use a igualdade $x^{(q-1)/2} + y^{(q-1)/2} + z^{(q-1)/2} = 0$, juntamente com $q > 5$, para chegar a uma contradição. Por fim, para (g) ii., observe que, se $q \mid a$ e $\text{mdc}\,(a, d) = 1$, então $q \nmid d$.

13. Para o item (e), você precisará utilizar o resultado do exemplo 3.14. Para o item (h), mostre primeiro que $q_n = 2^{n-1}q_1 + (2^{n-1} - 1)$, para todo inteiro $n \geq 1$; em seguida, use o pequeno teorema de Fermat para mostrar que, se q_1 for um primo ímpar, então é possível escolher $n \geq 2$ tal que $q_1 \mid q_n$.

Seção 5.3

1. Provemos os dois itens simultaneamente. Se x é um inteiro tal que $ax \equiv b \pmod n$, então temos $ax = nq+b$, para algum $q \in \mathbb{Z}$. Portanto, $b = xa + (-q)n$, uma combinação linear de a e n, e segue do teorema de Bézout que $\text{mdc}\,(a,n) \mid b$. Suponha, pois, que $\text{mdc}\,(a,n) = d$ e que $d \mid b$. Então
$$ax \equiv b \pmod n \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \left(\text{mod}\, \frac{n}{d}\right).$$
Mas, como $\text{mdc}\,\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, a existência de solução segue do corolário 5.25. Para o que falta, observe que
$$ax \equiv ax_0 \pmod n \Leftrightarrow x \equiv x_0 \left(\text{mod}\, \frac{n}{d}\right) \Leftrightarrow x = x_0 + \frac{n}{d}t,\ \exists\, t \in \mathbb{Z}.$$
Por outro lado, é imediato que
$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod n \Leftrightarrow t_1 \equiv t_2 \pmod d,$$
de maneira que há tantas soluções para a equação original incongruentes, módulo n, quantos forem os valores de t incongruentes, módulo d, i.e., a equação original tem exatamente $d = \text{mdc}\,(a,n)$ soluções incongruentes módulo n.

2. Se a congruência em questão possui solução, utilize o teorema de Bézout, juntamente com o item (d) da proposição 5.6, para mostrar que o mdc entre $\text{mdc}\,(a_1, a_2, \ldots, a_k)$ e n divide b. Em seguida, observe que
$$\text{mdc}\,(\,\text{mdc}\,(a_1, a_2, \ldots, a_k), n) = \text{mdc}\,(a_1, a_2, \ldots, a_k, n). \tag{8.1}$$

Para a recíproca, utilize novamente o teorema de Bézout, juntamente com 8.1).

3. Se x denota o número de soldados, mostre que x satisfaz um sistema de congruências lineares com duas equações. Em seguida, utilize a prova do teorema 5.27 para mostrar que $x \equiv 7 \cdot 12 \cdot 12 + 5 \cdot 1 \cdot 13 \pmod{12 \cdot 13}$ e, portanto, que $x = 132q + 17$, para algum $q \in \mathbb{Z}$. Por fim, utilize a condição $600 < x < 700$ para concluir que $x = 677$.

4. Para o item (a), comece observando que, se u, v for uma solução da equação Diofantina linear em questão e $x = m_1u + a_1 = m_2v + a_2$, então x resolve (5.7) para $k = 2$.

5. Use o teorema de Euler 5.19.

6. Se p e q são primos distintos, segue do exemplo 1.28 que $2^p - 1$ e $2^q - 1$ são primos entre si. De posse dessa observação, mostre que um inteiro x satisfaz as condições do enunciado se, e só se, resolver um sistema de congruências lineares apropriado. Por fim, aplique o teorema chinês dos restos.

7. Adapte, ao presente caso, a ideia da prova do exemplo 5.28.

8. Para a implicação $\Leftarrow$ do item (a), seja $a_i \in \mathbb{Z}$ uma solução de $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$. Se x for uma solução do sistema de congruências lineares
$$\begin{cases} x \equiv a_1 \pmod{p_1^{\alpha_1}} \\ x \equiv a_2 \pmod{p_2^{\alpha_2}} \\ \quad \cdots \\ x \equiv a_k \pmod{p_k^{\alpha_k}} \end{cases}$$
– cuja existência é garantida pelo teorema chinês dos restos –, use o item (c) da proposição 5.6 para concluir que $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$, para $1 \leq i \leq k$ e, daí, que $f(x) \equiv 0 \pmod m$. Para o item (b), seja $S(t)$ um conjunto de $N(t)$ soluções duas a duas incongruentes, módulo t, para a congruência $f(x) \equiv 0 \pmod t$. Use o resultado do item (a) para garantir a existência de uma bijeção $f : S(m) \to S(p_1^{\alpha_1}) \times \cdots \times S(p_k^{\alpha_k})$; em seguida, aplique o princípio fundamental da contagem.

9. Se a é o primeiro termo e r a razão da PA, as hipóteses do problema equivalem à existência de $x, y \in \mathbb{N}$, tais que $x^2 \equiv a \pmod{r}$ e $y^3 \equiv a \pmod{r}$; da mesma forma a tese do problema equivale à existência de $z \in \mathbb{N}$, tal que $z^6 \equiv a \pmod{r}$. Faça indução completa sobre r, sendo o caso $r = 1$ trivial; para o passo de indução, considere separadamente os casos $r = p^\alpha$, para algum primo p e algum $\alpha \in \mathbb{N}$, e $r = st$, com $s, t > 1$ primos entre si. No primeiro caso, se x e y são como no início e y' é o inverso de y, módulo p^α, mostre que $z = xy'$ satisfaz o problema. No segundo caso, sejam u e v termos das PA's $(a + ks)_{k \geq 0}$ e $(a + kt)_{k \geq 0}$, respectivamente, tais que $u^6 \equiv a \pmod{s}$ e $v^6 \equiv a \pmod{t}$; use o teorema chinês dos restos para encontrar $z \in \mathbb{N}$, tal que $z^6 \equiv a \pmod{st}$.

Seção 7.1

2. Por contradição, se $2^{3^n} \equiv -1 \pmod{17}$, então $2^{2 \cdot 3^n} \equiv 1 \pmod{17}$; use a congruência $2^{16} \equiv 1 \pmod{17}$, para concluir que $\text{ord}_{17}(2) = 1$ ou 2, o que é uma contradição.

3. Se $m = \text{ord}_n(a)$, então $m \mid 2k$ e, pelo teorema de Euler, m divide $\varphi(n)$. Portanto, $m \mid \text{mdc}(2k, \varphi(n)) = 2d$, onde $d = \text{mdc}(k, \varphi(n)/2)$ (recorde que $n > 2 \Rightarrow \varphi(n)$ par – cf. problema 19, página 88). Se $m \mid d$, então $m \mid k$, o que contradiz a congruência do enunciado. Logo, $m = 2d'$, para algum divisor d' de d e, daí, m é par.

4. Se $n \mid (2^n - 1)$, então n é ímpar; se $n > 1$ e $k = \text{ord}_n(2)$, então $1 < k \mid n, \varphi(n)$; escolha, de início, o menor natural $n > 1$ tal que $n \mid (2^n - 1)$ e chegue a uma contradição mostrando que $k \mid (2^k - 1)$, com $1 < k < n$.

5. Denote por S o produto do enunciado. Pela fórmula de Legendre (1.9), a maior potência de 2 que divide $n!$ tem expoente

$$e_2(n) = \sum_{j=1}^{+\infty} \left\lfloor \frac{n}{2^j} \right\rfloor < \sum_{j=1}^{+\infty} \frac{n}{2^j} = n,$$

temos $e_2(n) \leq n - 1$ e, daí, $2^{e_2(n)} \mid S$. Seja, agora, $2 < p \leq n$ primo e l o expoente da maior potência de p que divide S. Use o fato de $2^n - 2^t \equiv 0 \pmod{p^j}$ se, e só se, $\text{ord}_{p^j}(2) \mid (n - t)$, juntamente com a ideia da prova da fórmula de Legendre, para concluir que

$$l = \sum_{j \geq 1} \left\lfloor \frac{n}{\text{ord}_{p^j}(2)} \right\rfloor > \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor = e_p(n).$$

6. Mostre que $k_{i+1} \equiv 2k_i \pmod{2n+1}$. Em seguida, para o item (a), conclua que $f(n) = 0$ se, e só se, o conjunto $\{1, 2, 2^2, 2^3, \ldots\}$ contiver um SCI módulo $2n + 1$. Para o item (b), mostre que

$$f(1997) = 2 \cdot 1997 - \text{ord}_{2 \cdot 1997+1}(2)$$

e calcule $\text{ord}_{2 \cdot 1997+1}(2) = 8 \cdot 23 = 184$ utilizando as igualdades $2 \cdot 1997 + 1 = 5 \cdot 17 \cdot 47$, $\text{ord}_{17}(2) = 8$ e $\text{ord}_{47}(2) = 23$.

Seção 7.2

1. Mostre que $2^{14} \equiv -1 \pmod{29}$ e, a partir daí, conclua que $\text{ord}_{29}(2) = 28$.

2. Considere separadamente os casos $n = 2, 4, p^k$ e $2p^k$, com p primo ímpar e $k \in \mathbb{N}$.

3. Se a é uma raiz primitiva módulo n, observe que os números a_i são congruentes, em alguma ordem, aos números $a, a^2, \ldots, a^{\varphi(n)}$, de sorte que
$$a_1 a_2 \ldots a_{\varphi(n)} \equiv a^{\frac{\varphi(n)(\varphi(n)+1)}{2}} \pmod{n}.$$
Se $n = 2$ ou 4, mostre diretamente que $a^{\frac{\varphi(n)(\varphi(n)+1)}{2}} \equiv -1 \pmod{n}$; se $n = p^k$ ou $2p^k$, onde $k \in \mathbb{N}$ e p é um primo ímpar, use o fato de que $\text{ord}_n(a) = \varphi(n)$ para concluir que $a^{\frac{\varphi(n)}{2}} \equiv -1 \pmod{n}$ – cuidado: $n \mid (a^{\frac{\varphi(n)}{2}} + 1)(a^{\frac{\varphi(n)}{2}} - 1)$ não necessariamente implica diretamente que $n \mid (a^{\frac{\varphi(n)}{2}} + 1)$ ou $n \mid (a^{\frac{\varphi(n)}{2}} - 1)$.

4. Se $a^{3pq-1} \equiv 1 \pmod{3pq}$, então $a^{3pq-1} \equiv 1 \pmod{p}$; em particular, sendo a uma RP módulo p, devemos ter $(p-1) \mid (3pq-1)$ e, analogamente, $(q-1) \mid (3pq-1)$. Conclua, a partir daí, que $(p-1) \mid (3q-1)$ e $(q-1) \mid (3p-1)$, de modo que $p = 11$ e $q = 17$, ou vice-versa. Por fim, mostre que $a^{3 \cdot 11 \cdot 17 - 1} \equiv 1 \pmod{3 \cdot 11 \cdot 17}$, para todo natural a primo com $3 \cdot 11 \cdot 17$. Para mostrar que $p = 11$ e $q = 17$ se $p \leq q$, pode-se argumentar da seguinte maneira: como $p \leq q$, temos
$$\frac{3p-1}{q-1} \leq \frac{3q-1}{q-1} = 3 + \frac{2}{q-1} \leq 3 + \frac{2}{4},$$
de sorte que $\frac{3p-1}{q-1} = 1$, 2 ou 3; analisando cada caso separadamente, concluímos que $3p - 1 = 2(q-1)$ e, daí, $\frac{3q-1}{p-1} = \frac{9q-3}{2q-4}$, um número maior que 4 e menor que 8; assim, $\frac{9q-3}{2q-4} = 5$, 6 ou 7, o que fornece $q = 17$ como única possibilidade viável.

5. Para o item (d), considere separadamente os casos $\text{ord}_p(x) = 1$, 2, $\frac{p-1}{2}$ ou $p - 1$ – aqui usamos que $(p-1)/2$ também é primo.

6. Para (a) $\Rightarrow$ (b), escreva $n = p_1 \ldots p_k$, com $p_1 < \cdots < p_k$ números primos tais que $(p_i - 1) \mid (n-1)$; em seguida, use o pequeno teorema de Fermat para concluir que $a^n \equiv a \pmod{p_i}$, para todo $1 \leq i \leq k$. Para (b) $\Rightarrow$ (a), tome um divisor primo p de n e faça o inteiro a igual a uma RP módulo p^2 para obter uma contradição se $p^2 \mid n$; em seguida, faça o inteiro a igual a uma raiz primitiva módulo p, para concluir que $(p-1) \mid (n-1)$.

7. Para o item (a), observe que
$$\sum_{j=0}^{pq-1} \sum_{l=0}^{p-1} (pj + l)^{n-1} \equiv \sum_{j=0}^{pq-1} \sum_{l=0}^{p-1} l^{n-1} \equiv pq \cdot \sum_{l=0}^{p-1} l^{n-1} \equiv 0 \pmod{p}.$$
Para o item (b), use (a) para concluir que, se $n = p^2 q$, com p primo e q natural, então $s_n \equiv 1 \pmod{p}$. O item i. é um cálculo análogo àquele indicado na sugestão de (a). O item ii. segue imediatamente de i., juntamente com o fato de que, módulo p_i, temos $\{a, a^2, \ldots, a^{p_i - 1}\} = \{1, 2, \ldots, p_i - 1\}$. Para iii., se $n \mid s_n$, então $s_n \equiv 0 \pmod{p_i}$. Mas, como $p_i \mid (a^{p_i(n-1)} - a^{n-1})$, a fórmula em ii. garante que a única maneira de $s_n \equiv 0 \pmod{p_i}$ é que $p_i \mid (a^{n-1} - 1)$. Então, $p_i - 1 = \text{ord}_{p_i}(a) \mid (n-1)$ e, daí, $(p_i - 1) \mid (q_i - 1)$(uma vez que $n - 1 = (p_i - 1)q_i + (q_i - 1)$). Para iv., se $n \mid s_n$, então $p_i \mid s_n$, e segue de i. e iii. (especificamente, de $(p_i - 1) \mid (n-1)$) que, módulo p_i,
$$0 \equiv s_n = 1 + q_i \sum_{l=1}^{p_i - 1} l^{n-1} \equiv 1 + q_i \sum_{l=1}^{p_i - 1} 1 \equiv 1 + q_i(p_i - 1);$$
portanto, $q_i(p_i - 1) \equiv -1 \equiv p_i - 1 \pmod{p_i}$, de sorte que $q_i \equiv 1 \pmod{p_i}$. Por fim, em relação ao item v., é suficiente mostrar que, se $p_i(p_i - 1) \mid (q_i - 1)$ para $1 \leq i \leq t$, então $p_i \mid s_n$, para $1 \leq i \leq t$; para tanto, basta utilizar a congruência do item i., juntamente com o fato (facilmente dedutível a partir de nossas hipóteses) de que $(p_i - 1) \mid (n-1)$.

8. Para o item (a), se $\text{mdc}(a^k + 1, n) > 1$, então $n \mid (a^k + 1)$ e, daí, $a^{2k} \equiv 1 \pmod{n}$, o que contradiz o fato de $\text{ord}_n(a) = 2pk$. Para

i., segue de $a^{kp} \equiv -1 \pmod{n}$ que $a^{2kp} \equiv 1 \pmod{n}$, de sorte que $d \mid 2kp = n-1$. Por outro lado, se $d \mid 2k$, então $a^{2k} \equiv 1 \pmod{n}$ e, assim, $n \mid (a^k-1)(a^k+1)$; mas, como $\text{mdc}\,(a^k+1, n) = 1$, segue daí que $n \mid (a^k-1)$ e, portanto, $a^{kp} \equiv 1 \pmod{n}$, um absurdo. Agora, se $d \mid 2kp$ e $d \nmid 2k$, é imediato que $\text{mdc}\,(d,p) > 1$, de sorte que $p \mid d$; então, a última parte de i. segue do teorema de Euler. Quanto a ii., é evidente que $p \nmid (2kp+1)$; portanto, a fórmula para $\varphi(2kp+1)$ garante que $p \mid (q-1)$, para algum divisor primo q de $2kp+1$; logo, basta fazer $q - 1 = lp$, observando que $l > 1$ pois, do contrário, tanto p quanto $q = p+1$ seriam primos ímpares, o que é um absurdo. Por fim, para iii., se $2kp + 1 = (lp+1)u$, então $u \equiv 1 \pmod{p}$, de maneira que $u = hp + 1$, para algum $h \geq 1$; se $h \geq 2$, então $n = (lp+1)(hp+1) \geq (2p+1)^2 > 2(2p+1)p + 1 \geq 2kp + 1 = n$, um absurdo; logo, $h = 0$ ou 1 e, se $h = 1$, então $(p+1) \mid (2kp+1)$, o que é um absurdo (pois $p+1$ é par e $2kp+1$ é ímpar.

9. O item (a) segue do pequeno teorema de Fermat, juntamente com o fato de que $x_1^4+x_2^4+x_3^4+x_4^4+x_5^4 \equiv 0 \pmod{p}$ se, e só se, $f(x_1, \ldots, x_5) \equiv 1 \pmod{p}$. O item (b) segue da fórmula do desenvolvimento multinomial (cf. problema 1.4.2 do volume 4) e do resultado do item (a).

Seção 7.3

1. Use o critério de Euler.

2. Adapte a prova do exemplo 7.24 ao presente caso para obter infinitos valores de k com a propriedade desejada.

3. Comece multiplicando a igualdade do enunciado por $4a$ e completando quadrados.

4. Mostre inicialmente que, se existirem tais x e y, então eles são primos com 122. Use, então, o resultado do problema anterior para concluir que 17 é resíduo quadrático módulo 61. Por fim, aplique a lei da reciprocidade quadrática e a proposição 7.23 para chegar a uma contradição.

5. Para o item (a), se todo divisor primo de $2b^2+3$ fosse congruente a ± 1, módulo 8, teríamos $2b^2 + 3 \equiv \pm 1 \pmod{8}$; mostre que isso é impossível. Para o item (b), se $(2b^2+3) \mid (a^2-2)$ e p é como em (a), então $a^2 \equiv 2 \pmod{p}$, i.e., 2 seria um resíduo quadrático, módulo p; use o resultado do exemplo 7.26 para chegar a uma contradição.

6. Aplique o lema de Gauss, nos moldes do exemplo 7.26, ou a lei da reciprocidade quadrática.

7. Para o item (a), se todo divisor primo de $2^n - 1$ fosse congruente a ± 1, módulo 12, teríamos $2^n - 1 \equiv \pm 1 \pmod{12}$; mostre que isso é impossível. Para o item (b), se $(2^n - 1) \nmid (3^m - 1)$ e p é como em (a), então $3^m \equiv 1 \pmod{p}$ ou, ainda, $3^{m+1} \equiv 3 \pmod{p}$; como $m+1$ é par, seguiria que 3 seria um resíduo quadrático, módulo p; use o resultado do problema anterior para chegar a uma contradição.

8. Para o item (a), use a lei da reciprocidade quadrática. Para o item (b), use o resultado do corolário 7.20, juntamente com o fato de que $p-1$ é uma potência de 2.

9. Para o item (a) faça indução sobre $k \geq 3$, mostrando que, se $x_k^2 \equiv a \pmod{2^k}$, então $x_{k+1}^2 \equiv a \pmod{2^{k+1}}$, com $x_{k+1} = x_k$ ou $x_k + 2^{k-1}$. Para o item (b) faça uma indução análoga; mais precisamente, se $x_k^2 = p^k q + a$, faça $x_{k+1} = x_k + p^k t$, com $t \in \mathbb{Z}$, e imponha a validade da congruência $x_{k+1}^2 \equiv a \pmod{p}$ para deduzir que t deve satisfazer a congruência linear $2x_k t \equiv -q \pmod{p}$; por fim, mostre que é sempre possível escolher um tal t.

10. Se $x^2 \equiv a \pmod{n}$ para um certo inteiro x, então $x^2 \equiv a \pmod{2^k}$ e $x^2 \equiv a \pmod{p_i^{k_i}}$, para $1 \leq i \leq t$; basta, pois, aplicar os resultados do problema anterior, juntamente com o critério de Euler. Reciprocamente, uma vez satisfeitas as condições (i) e (ii), aplique novamente os resultados do problema anterior, juntamente com o critério de Euler, para garantir a existência de inteiros $x_0, x_1, \ldots, x_t$ tais que

$x_0^2 \equiv a \pmod{2^k}$ e $x_i^2 \equiv a \pmod{p_i^{k_i}}$, para $1 \leq i \leq t$; por fim, aplique o teorema chinês dos restos para obter, a partir dos x_i's, um inteiro x que satisfaça todas essas congruências simultaneamente.

11. Numere as crianças no sentido horário e de maneira *contínua*, de forma que o professor encontre a primeira criança nas posições 1, $n+1$, $2n+1$, $3n+1$, ..., e analogamente para as demais crianças. Mostre que o professor entregará doces às crianças nas posições $\frac{k(k+1)}{2}$, para $k \in \mathbb{N}$, de sorte que basta encontrarmos os valores de n tais que a congruência $\frac{x(x+1)}{2} \equiv a \pmod{n}$ tenha solução, para todo inteiro $1 \leq a \leq n$. Em seguida, observe que, se tal congruência tem solução, então o mesmo sucede com a congruência $(2x+1)^2 \equiv 8a+1 \pmod{n}$, e use o problema 10 para mostrar que n tem de ser uma potência de 2.

12. Para $\Rightarrow$, use o pequeno teorema de Fermat. Para $\Leftarrow$, sejam α uma raiz primitiva, módulo p, e $j \in \mathbb{N}$ tal que $\frac{n}{d}j \equiv -1 \left(\bmod \frac{p-1}{d}\right)$; em seguida, tome $k \in \mathbb{N}$ tal que $\alpha^k \equiv a^j \pmod{p}$ e mostre que $k \mid d$ e $x_0 = \alpha^{k/d}$ resolve a congruência $x^n \equiv a \pmod{p}$.

13. Os itens de (a) a (d) utilizam somente manipulações algébricas simples e propriedades elementares de congruências. Para a primeira parte do item (e), use o teorema de Wilson, juntamente com o critério de Euler; para a segunda parte, suponha, por contradição, que $r_i \equiv r_j \pmod{p}$ e use o fato de que $p \nmid (j^2 - i^2)$. Para a segunda parte do item (f), conclua que

$$\sum_{j=1}^{\frac{p-1}{2}} r_j \equiv \sum_{j=1}^{\frac{p-1}{2}} j^2 \equiv 0 \pmod{p},$$

onde, na última congruência, utilizamos o fato de que $p \geq 5$.

Seção 7.4

1. Com o auxílio da proposição 5.9 mostre que, se existissem inteiros k, l, x, y e z como no enunciado, com $l \geq 1$, então x, y e z seriam todos pares.

2. Suponha, por contradição, que $a+b$ é par. Então, $a + c^2 = a^2 - b^2 \equiv 0 \pmod{4}$, de sorte que $a \equiv -c^2 \pmod{4}$. Conclua, a partir daí, que $a(a-1)$ tem um fator primo congruente a 3 módulo 4 que aparece com expoente ímpar em sua decomposição canônica.

3. Observe que $1995 = 3 \cdot 5 \cdot 7 \cdot 19$, com $3, 7, 19 \equiv 3 \pmod{4}$. Por outro lado, se d é um divisor positivo de 1995 (o caso $d < 0$ pode ser tratado de forma totalmente análoga), analise separadamente as quatro possibilidades a seguir: $d = 1$, $d = 5$, $1 < d \mid (3{\cdot}7{\cdot}19)$ e $d = 5d'$, onde $1 < d' < (3 \cdot 7 \cdot 19)$, de acordo com os seguintes exemplos: (i) se $d = 5$, então $x^2 + y^2 = 5(x-y)$ se, e só se, $(2x-5)^2 + (2y+5)^2 = 50$, de forma que $2x - 5 = \pm 1, \pm 7$; (ii) se $1 < d \mid (3 \cdot 7 \cdot 19)$, então, como $x^2 + y^2 \equiv 0 \pmod{d}$, o argumento esboçado no passo (ii) da demonstração do teorema 7.32 garante que $d \mid x$ e $d \mid y$; pondo $x = da$ e $y = db$, obtemos $a^2 + b^2 = a - b$, a qual equivale à primeira das quatro possibilidades acima.

4. O exemplo 1.39 garante a existência de infinitos primos da forma $4k+3$; escolha, então, n primos $q_1, \ldots, q_n$, todos congruentes a 3 módulo 4, e aplique o teorema chinês dos restos, juntamente com o teorema 7.32, ao sistema de congruências lineares $x \equiv -i + q_i \pmod{q_i^2}$, para $1 \leq i \leq n$.

5. Para o item (d), use a identidade (7.9).

6. Para o item (a), suponha que n tem um divisor ímpar $d > 1$. Então, como $(2^d - 1) \mid (2^n - 1)$, temos que $(2^d - 1) \mid (m^2 + 9)$, o qual é uma soma de dois quadrados perfeitos. Contudo, como $2^d - 1$ é da forma $4k - 1$, ele deve ter algum divisor primo p dessa forma. Segue, agora, da discussão da teoria desta seção que $p \mid m$ e $p \mid 3$,

de forma que $p = 3$. Logo, $3 \mid (2^d - 1)$, o que é um absurdo, já que $2^d - 1 \equiv (-1)^d - 1 \equiv -2 \pmod 3$. Para o item (b), comece observando que o caso $k = 1$ é trivial. Agora, suponha que $(2^{2^{k-1}} - 1) \mid (m_{k-1}^2 + 9)$ e observe que $(2^{2^{k-1}} + 1) \mid ((3 \cdot 2^{2^{k-2}})^2 + 9)$. Em seguida, escolha, com o auxílio do teorema chinês dos restos, $m_k \in \mathbb{N}$ tal quer

$$m_k \equiv m_{k-1} \pmod{2^{2^{k-1}} - 1} \text{ e } m_k \equiv 3 \cdot 2^{2^{k-2}} \pmod{2^{2^{k-1}} + 1}.$$

É imediato verificar que $2^{2^{k-1}} - 1$ e $2^{2^{k-1}} + 1$ dividem $m_k^2 + 9$; mas, como tais fatores são primos entre si, concluímos que seu produto também divide $m_k^2 + 9$.

Referências

[1] AIGNER, M. e ZIEGLER, G. (2010) *Proofs from THE BOOK.* Springer-Verlag.

[2] ANDREWS, G. (1994). *Number Theory.* Dover.

[3] APOSTOL, T. (1976). *Introduction to Analytic Number Theory.* Springer-Verlag.

[4] DE FIGUEIREDO, D. G. (1987). *Análise de Fourier e Equações Diferenciais Parciais.* Instituto Nacional de Matemática Pura e Aplicada.

[5] LANDAU, E. (2002). *Teoria Elementar dos Números.* Ciência Moderna.

[6] LIMA, H. N. (2011). *Limites e Funções Aritméticas.* Preprint.

[7] ROBERTS, J. (1978). *Elementary number theory: a problem oriented approach.* MIT Press.

[8] SCHEINERMAN, E. (2010). *Matemática Discreta, uma Introdução.* Cengage Learning.

[9] SINGH, S. (1998). *O Último Teorema de Fermat.* Record.

[10] STEIN, E. e SHAKARCHI, R. (2003). *Fourier Analysis. An Introduction.* Princeton University Press.

[11] VAINSENCHER, I. (1996). *Introdução às Curvas Algébricas Planas.* Instituto Nacional de Matemática Pura e Aplicada.

CAPÍTULO A

Glossário

APMO: Asian-Pacific Mathematical Olympiad.

Áustria-Polônia: Olimpíada de Matemática Austro-Polonesa.

BMO: Balkan Mathematical Olympiad.

Baltic Way: Baltic Way Mathematical Contest.

Crux: Crux Mathematicorum, periódico de problemas da Sociedade Canadense de Matemática.

IMO: International Mathematical Olympiad.

Israel-Hungria: Competição Binacional Israel-Hungria.

Miklós-Schweitzer: The Miklós-Schweitzer Mathematics Competition (Hungria).

NMC: Nordic Mathematical Contest.

OBM: Olimpíada Brasileira de Matemática.

OBMU: Olimpíada Brasileira de Matemática para Universitários.

OCM: Olimpíada Cearense de Matemática.

OCS: Olimpíada de Matemática do Cone Sul.

OIM: Olimpíada Ibero-americana de Matemática.

OIMU: Olimpíada Ibero-americana de Matemática Universitária.

ORM: Olimpíada Rioplatense de Matemática.

Putnam: The William Lowell Mathematics Competition (Estados Unidos).

Torneio das Cidades: The Tournament of the Towns, olimpíada intermunicipal mundial de Matemática.

Índice Remissivo

Algoritmo
  da divisão, 5
  de Euclides, 24

Bézout
  Étienne, 14
  teorema de, 14

Cesàro, Ernesto, 105
Chebyshev
  Pafnuty, 92
  teorema de, 102
Chevalley
  teorema de, 186
Chevalley, Claude, 186
Classe
  de congruência, 153
Congruência
  classe de, 153
  como relação de equivalência, 120
  propriedades elementares da, 120
  relação de, 153
Congruências
  lineares, 145
Cubo perfeito, 12

Decomposição canônica de um inteiro, 42
Descida de Fermat, 55
Diofanto de Alexandria, 22
Dirichlet
  Gustav L., 39, 64
  lema de, 64
Divisão
  algoritmo da, 5
  quociente de uma, 5
  resto de uma, 5
Divisibilidade
  por 11, critério de, 10

por 9, critério de, 10, 122
propriedades elementares da, 3
relação de, 1
Divisor
comum, 13
comum, máximo, 13
de um inteiro, 2
positivo, 2

Eisenstein
Ferdinand, 196
Equação
de Fermat, 56
de Pítágoras, 51
de Pell, 63
Diofantina, 22
diofantina linear, 23
Eratóstenes
crivo de, 37
de Cirene, 38
teorema de, 36
Espaço amostral, 105
Euclides
algoritmo de, 24
lema de, 36
teorema de, 37
Euler
critério de, 189
função φ de, 81
identidade de, 204
teorema de, 62, 82, 85, 96, 136, 160, 207
Evento, 106

Fórmula
de inversão de Möbius, 79
de Legendre, 45
para $\varphi(n)$, 82
Fermat
descida de, 55
equação de, 56
grande teorema de, 56
número de, 13
pequeno teorema de, 134
Pierre Simon de, 52
teorema de, 202, 204
Fração irredutível, 17
Função
φ de Euler, 81
aritmética, 73
aritmética multiplicativa, 73
de Euler, fórmula para a, 82
de Euler, multiplicatividade da, 82
de Möbius, 77
número de divisores positivos, 74
soma de divisores positivos, 76

Gauss
lei da reciprocidade quadrática de, 196
lema de, 192

Hadamard
Jacques, 92
teorema de, 92

Identidade
de Euler, 204
Inteiro
divisível por outro, 2
divisor de um, 2
livre de quadrados, 47
múltiplo de um, 2
mais próximo, 12
Inteiros
congruentes, 118
primos entre si, 13
relativamente primos, 13
Inverso
multiplicativo, 164
Inverso módulo n, 145

Lagrange
Joseph L., 207
teorema de, 207
Lamé
teorema de, 35
Lamé, Gabriel, 35
Legendre
Adrien-Marie, 45
fórmula de, 45
símbolo de, 190
Lema
de Dirichlet, 64
de Euclides, 36
de Gauss, 192
Liouville
Joseph, 86
teorema de, 86

Möbius
fórmula de inversão de, 79
função de, 77
Máximo divisor comum, 13
Múltiplo
comum, mínimo, 28
de um inteiro, 2
Mínimo múltiplo comum, 28
mmc, 28

Número
ímpar, 2
abundante, 86
composto, 35
de Fermat, 13
par, 2
perfeito, 85
primo, 35
primo, teorema do, 92

Ordem módulo n, 170

Parte fracionária, 64
Parte inteira, 5
Pell
equação de, 63
John, 63
Pitágoras

equação de, 51
Pitágoras de Samos, 53
Primo, 35
Probabilidade, 105
distribuição de, 105

Quadrado perfeito, 6
Quociente, 5

Raiz
de uma congruência, 145
Raiz primitiva
módulo n, 175
Relação
de congruência, 153
de divisibilidade, 1
Resíduo
$n-$ésimo módulo p, 201
quadrático módulo n, 188
Resto, 5

SCR, 154
Sistema
completo de invertíveis, 158
completo de restos, 154
Soma dos divisores positivos, 77

Taylor, Richard, 56
Teorema
chinês dos restos, 148
de Bézout, 14
de Chebyshev, 102
de Chevalley, 186
de Eratóstenes, 36
de Euclides, 37
de Euler, 62, 82, 85, 96, 136, 160, 207
de Fermat, 202, 204
de Fermat, grande, 56
de Fermat, pequeno, 134
de Hadamard, 92
de Lagrange, 207
de Lamé, 35
de Liouville, 86
de Sophie Germain, 143
de Wilson, 146
de Wilson, generalização do, 184
do número primo, 92
fundamental da aritmética, 41
Terno Pitagórico, 53

Unidade
em $\mathbb{Z}_n$, 164

Wiles, Andrew, 56
Wilson
generalização do teorema de, 184
teorema de, 146

(continuação dos títulos publicados)

- *Elementos de Topologia Geral* - E. L. Lima
- *A Construção dos Números* - J. Ferreira
- *Introdução à Geometria Projetiva* - A. Barros e P. Andrade
- *Análise Vetorial Clássica* - F. Acker
- *Funções, Limites e Continuidade* - P. Ribenboim
- *Fundamentos de Análise Funcional* - D. Pellegrino, E. Teixeira e G. Botelho
- *Teoria dos Números Transcendentes* - D. Marquez
- *Introdução à Geometria Hiperbólica* - O modelo de Poincaré - P. Andrade

COLEÇÃO MATEMÁTICA APLICADA

- *Introdução à Inferência Estatística* - H. Bolfarine e M. Sandoval
- *Discretização de Equações Diferenciais Parciais* - J. Cuminato e M. Meneguette

COLEÇÃO OLIMPÍADAS DE MATEMÁTICA

- *Olimpíadas Brasileiras de Matemática, 1a a 8a* - E. Mega, R. Watanabe
- *Olimpíadas Brasileiras de Matemática, 9a a 16a* - C. Moreira, E. Motta, E. Tengan, L. Amâncio, N. C. Saldanha e P. Rodrigues
- *21 Aulas de Matemática Olímpica* - C. Y. Shine
- *Iniciação à Matemática: Um curso com problemas e soluções* - K. I. M. Oliveira e A. J. C. Fernández

COLEÇÃO FRONTEIRAS DA MATEMÁTICA

- *Fundamentos da Teoria Ergódica* - M.Viana e K. Oliveira